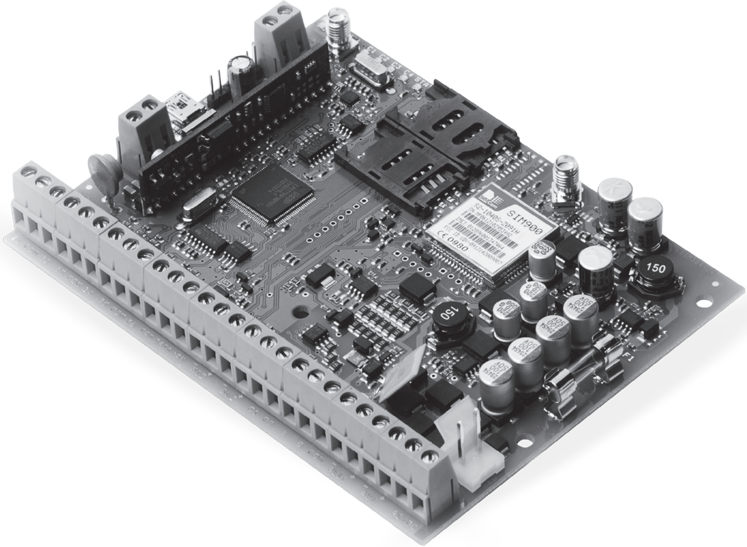


eldes

ESIM364

GSM ALARM AND MANAGEMENT SYSTEM

INSTALLATION MANUAL

COMPLIES WITH EN 50131-1 GRADE 3, CLASS II REQUIREMENTS

Installation Manual v1.6
Valid for ESIM364 v02.07.00 and up

Safety instructions

Please read and follow these safety guidelines in order to maintain safety of operators and people around:

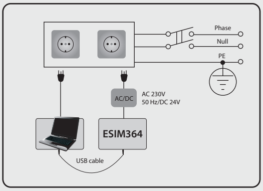
- GSM alarm & management system ESIM364 (also referenced as alarm system, system or device) has radio transceiver operating in GSM 850/900/1800/1900 bands.
- DO NOT use the system where it can be interfere with other devices and cause any potential danger.
- DO NOT use the system with medical devices.
- DO NOT use the system in hazardous environment.
- DO NOT expose the system to high humidity, chemical environment or mechanical impacts.
- DO NOT attempt to personally repair the system.
- System label is on the bottom side of the device.

GSM alarm system ESIM364 is a device mounted in limited access areas. Any system repairs must be done only by qualified, safety aware personnel.

The system must be powered by main 16-24V 50 Hz ~1.5A max or 18-24V ⎓ 1,5A max DC power supply which must be approved by LST EN 60950-1 standard and be easily accessible nearby the device. When connecting the power supply to the system, switching the pole terminals places does not have any affect.

Any additional devices linked to the system ESIM364 (computer, sensors, relays etc.) must be approved by LST EN 60950-1 standard.

Main power supply can be connected to AC mains only inside installation room with automatic 2-pole circuit breaker capable of disconnecting circuit in the event of short circuit or over-current condition. Open circuit breaker must have a gap between connections of more than 3mm and the disconnection current 5A.



Mains power and backup battery must be disconnected before any installation or tuning work starts. The system installation or maintenance must not be done during stormy conditions

Backup battery must be connected via the connection which in the case of breaking would result in disconnection of one of battery pole terminals. Special care must be taken when connecting positive and negative battery terminals. Switching the pole terminals places is NOT allowed.

In order to avoid fire or explosion hazards the system must be used only with approved backup battery.

The device is fully turned off by disconnecting 2-pole switch off device of the main power supply and disconnecting backup battery connector.

Fuse F1 type – Slow Blown 3A. Replacement fuses have to be exactly the same as indicated by the manufacturer.

If you use I security class computer for setting the parameters it must be connected to earth.

The WEEE (Waste Electrical and Electronic Equipment) marking on this product (see left) or its documentation indicates that the product must not be disposed of together with household waste. To prevent possible harm to human health and/or the environment, the product must be disposed on in an approved and environmentally safe recycling process. For further information on how to dispose of this product correctly, contact the system supplier, or the local authority responsible for waste disposal in your area.

Contents

Limited Liability

The buyer must agree that the system will reduce the risk of fire, theft, burglary or other dangers but does not guarantee against such events.

“ELDES UAB” will not take any responsibility regarding personal or property or revenue loss while using the system.

“ELDES UAB” liability according to local laws does not exceed value of the purchased system. “ELDES UAB” is not affiliated with any of the cellular providers therefore is not responsible for the quality of cellular service.

Manufacturer Warranty

The system carries a 24-month warranty by the manufacturer “ELDES UAB”. Warranty period starts from the day the system has been purchased by the end user. The warranty is valid only if the system has been used as intended, following all guidelines listed in the manual and within specified operating conditions. Receipt must be kept as a proof of purchase date.

The warranty is voided if the system has been exposed to mechanical impact, chemicals, high humidity, fluids, corrosive and hazardous environments or other force majeure factors.

Package Content

1. ESIM364	qty. 1
2. Microphone	qty.1
3. SMA antenna	qty. 2
4. Buzzer	qty. 1
5. Back-up battery connection wire...	qty. 1
6. User manual	qty. 1
7. Resistors 5,6kΩ	qty. 12
8. Resistors 3,3kΩ	qty. 6
9. Plastic standoffs	qty. 4

About Installation Manual

This document describes detailed installation and operation process of alarm system ESIM364. It is very important to read the installation manual before starting to use the system.

It is not allowed to copy and distribute information in this document or pass to a third party without advanced written authorization by “ELDES UAB”. “ELDES UAB” reserves the right to update or modify this document and/or related products without a warning. Hereby, “ELDES UAB” declares that this GSM alarm and management system ESIM364 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at www.eldes.lt

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

15.105 statement (for digital devices)

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be located or operating in conjunction with any other antenna or transmitter..

1. GENERAL INFORMATION

1.1. Functionality

ESIM364 – micro-controller based alarm system for houses, cottages, country homes, garages and other buildings, also capable of managing electrical appliances via cellular GSM/GPRS network. It can also be used as Intercom system.

Examples of using the system:

- Property security.
- Alarm switch.
- Thermostat, heating and air-conditioner control, temperature monitoring.
- Lighting, garden watering, water pump and other electrical equipment control via SMS text messages.
- Remote listening to what is happening in the secured area.
- Mains power status notification by SMS text message.
- Two-way intercom device via GSM network.

1.2. Compatible Device Overview

Wired Devices

Device	Description	Max. Connectable Devices
EKB2	LCD keypad	4*
EKB3	LED keypad	4*
EA1	Audio output module with 3,5mm jack	1**
EA2	Audio amplifier module 1W 8Ω	1**
EPGM1	16 zone and 2 PGM output expansion module	2
ELAN3-ALARM	Ethernet communicator	1
EPGM8	8 PGM output expansion module	1**

Wireless Devices

Device	Description	Max. Connectable Devices
EW1	Wireless 2 zone and 2 PGM output expansion module	32***
EW1B	Battery-powered wireless 2 zone and 2 PGM output expansion module	32***
EWP1	Wireless motion detector	32***
EWD1	Wireless magnetic door contact	32***
EWD2	Wireless magnetic door contact/shock sensor/water sensor	32***
EWK1****	Wireless keyfob with 4 buttons	5***
EWK2****	Wireless keyfob with 4 buttons	5***
EWS1	Wireless indoor siren	32***
EWK2A***	Wireless keyfob with 1 button	5***
EWS2	Wireless outdoor siren	32***
EKB3W	Wireless LED keypad	4***
EWF1	Wireless smoke detector	32***
EWS3	Wireless indoor siren	32***

* - A mixed combination of EKB2 and EKB3 keypads is supported. The combination can consist of up to 4 keypads in total.
** - Only 1 of these modules can be connected at a time if the module slots are implemented in ESIM364 unit.
*** - A mixed combination of wireless devices is supported. The combination can consist of up to 32 wireless devices in total.
**** - A mixed combination of EWK1 and EWK2 keyfobs is supported. The combination can consist of up to 5 keyfobs in total.

1.3. Default Parameters & Ways of Parameter Configuration

Main Settings

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
User 1... 10 name	N/A				✓
User 1... 10 phone number	N/A	✓	✓	✓	✓
User 1... 10 partition	Partition 1		✓	✓	✓
User 1...10 - call in case of alarm	Enabled		✓	✓	✓
Allow control from any phone number	Disabled	✓	✓	✓	✓
SMS password	0000	✓	✓	✓	✓
SMS language	Depends on the firmware				
Partition 1 name	PART1				✓
Partition 2 name	PART2				✓
Partition 3 name	PART3				✓
Partition 4 name	PART4				✓

Partition 1… 4 exit delay	15 seconds	✓	✓	✓	✓
GSM signal loss indication - delay	180 seconds				✓
GSM signal loss indication – activate output	N/A				✓
Dual SIM management – SIM card switch	Disabled				✓
Dual SIM management – try to find operator for a maximum of	3 time (s)				✓
Dual SIM management – send SMS/call via	Currently in use SIM				✓

Main Settings					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
Passwords/Codes					
Installer's code	1470		✓	✓	✓
Duress code	N/A		✓	✓	✓
SGS code	N/A		✓	✓	✓
Passwords/codes format	4-digit				✓
Prompt additionally for master code when configuring via keypad/software	Disabled				✓
Master code	1111		✓	✓	✓
Master code name	N/A				✓
Master code partition	Partition 1, Partition 2, Partition 3, Partition 4		✓	✓	✓
User code 2… 30	N/A		✓	✓	✓
User code 2… 30 name	N/A				✓
User code 2… 30 partition	Partition 1		✓	✓	✓
Faults					
Main power loss	Enabled				✓
Low battery	Enabled				✓
Battery dead or missing	Enabled				✓
Battery failed	Enabled				✓
Siren failed	Enabled				✓
Tamper alarm	Enabled				✓
Date/time not set	Enabled				✓
GSM connection failed	Enabled				✓
GSM antenna failed	Enabled				✓
Wireless antenna failed	Enabled				✓
Keypad lost	Enabled				✓
Notifications					
System armed – User 1… 10	Enabled		✓	✓	✓
System armed – SMS delivery report	Enabled		✓	✓	✓
System disarmed – User 1… 10	Enabled		✓	✓	✓
System disarmed – SMS delivery report	Enabled		✓	✓	✓
General alarm – User 1… 10	Enabled		✓	✓	✓
General alarm – SMS delivery report	Enabled		✓	✓	✓
Main power loss/restore – User 1… 10	Enabled		✓	✓	✓
Main power loss/restore – SMS delivery report	Enabled		✓	✓	✓
Battery failed – User 1… 10	Enabled		✓	✓	✓
Battery failed – SMS delivery report	Enabled		✓	✓	✓
Battery dead or missing – User 1… 10	Enabled		✓	✓	✓
Battery dead or missing – SMS delivery report	Enabled		✓	✓	✓
Low battery – User 1… 10	Enabled		✓	✓	✓
Low battery – SMS delivery report	Enabled		✓	✓	✓
Siren fail/restore – User 1… 10	Disabled		✓	✓	✓
Siren fail/restore – SMS delivery report	Disabled		✓	✓	✓
Date/time not set – User 1… 10	Disabled		✓	✓	✓
Date/time not set – SMS delivery report	Disabled		✓	✓	✓
GSM connection failed – User 1… 10	Disabled		✓	✓	✓
GSM connection failed – SMS delivery report	Disabled		✓	✓	✓
GSM antenna fail/restore – User 1… 10	Disabled		✓	✓	✓

GSM antenna fail/restore – SMS delivery report	Disabled		✓	✓	✓
Tamper alarm/restore – User 1... 10	Enabled		✓	✓	✓
Tamper alarm/restore – SMS delivery report	Enabled		✓	✓	✓
Keypad loss/restore – User 1... 10	Enabled		✓	✓	✓
Keypad loss/restore – SMS delivery report	Enabled		✓	✓	✓
Temperature info – User 1... 10	Enabled		✓	✓	✓
Temperature info – SMS delivery report	Enabled		✓	✓	✓
System started – User 1... 10	Enabled		✓	✓	✓
System started – SMS delivery report	Enabled		✓	✓	✓
Periodical info – User 1... 10	Enabled		✓	✓	✓
Periodical info – SMS delivery report	Enabled		✓	✓	✓
Wireless signal loss – User 1... 10	Enabled		✓	✓	✓
Wireless signal loss – SMS delivery report	Enabled		✓	✓	✓
Unable to arm – User 1... 10	Enabled		✓	✓	✓
Unable to arm – SMS delivery report	Enabled		✓	✓	✓
Send to all users simultaneously – all notifications	Disabled		✓	✓	✓
Time Synchronization					
Time synchronization over GSM network	Disabled				✓
Phone number of the currently inserted SIM card	N/A				✓
Synchronization frequency	30 days				✓
Event Log					
Event log	Enabled	✓	✓	✓	✓

Zones					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
On Board					
Z1... Z6 zone name	Zone1... Zone6	✓			✓
Z1 type	Delay		✓	✓	✓
Z2... Z6 type	Instant		✓	✓	✓
Z1... Z6 delay, ms	800 milliseconds				✓
Z1... Z6 – Stay	Disabled		✓	✓	✓
Z1... Z6 – Force	Disabled		✓	✓	✓
Z1... Z6 tamer name	Tamper1... Tamper6				✓
Delay-type zone – entry delay	15 seconds	✓	✓	✓	✓
Z1... Z6 partition	Partition 1		✓	✓	✓
Z1... Z6 – Shared	Disabled				✓
Z1... Z6 – audio track	N/A				✓
Delay becomes Instant in STAY mode	Disabled				
Chime	Enabled		✓	✓	✓
ATZ mode	Disabled		✓	✓	✓
Arm-disarm by zone No1... No4	N/A		✓	✓	✓
Zone connection type	Type 1		✓	✓	✓
EPGM1 Module					
Zone name	Zone X	✓			✓
Status	Enabled	✓	✓	✓	✓
Type	Instant		✓	✓	✓
Delay, ms	800 milliseconds				✓
Stay	Disabled		✓	✓	✓
Force	Disabled		✓	✓	✓
Tamper name	Tamper X				✓
Delay-type zone – entry delay	15 seconds		✓	✓	✓
Partition	Partition 1		✓	✓	✓
Shared	Disabled				✓
Audio track	N/A				✓
Wireless Devices					
Zone name	Zone X	✓			✓
Status	Enabled	✓	✓	✓	✓

Type	Depends on the connected wireless device model		✓	✓	✓
Stay	Disabled		✓	✓	✓
Force	Disabled		✓	✓	✓
Tamper name	Tamper X				✓
Delay-type zone – entry delay	15 seconds		✓	✓	✓
Partition	Partition 1		✓	✓	✓
Shared	Disabled				✓
Audio track	N/A				✓
Keypads					
Zone name	Zone X	✓			✓
Status	Disabled	✓	✓	✓	✓
Type	Instant		✓	✓	✓
Stay	Disabled		✓	✓	✓
Force	Disabled		✓	✓	✓
Tamper name	Tamper X				✓
Delay-type zone – entry delay	15 seconds		✓	✓	✓
Partition	Partition 1		✓	✓	✓
Shared	Disabled				✓
Audio track	N/A				✓
Virtual Zones					
Zone name	Zone X				✓
Status	Disabled			✓	✓
Type	Instant			✓	✓
Force	Disabled			✓	✓
Delay-type zone – entry delay	15 seconds			✓	✓
Partition	Partition 1			✓	✓
Shared	Disabled				✓

PGM Outputs

Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
On Board					
C1... C4 output name	Controll1... Controll4	✓			✓
Status	Turned OFF	✓	✓	✓	✓
Using module EPGM8	Disabled		✓	✓	✓
EPGM1 Module					
Output name	ControllX	✓			✓
Status	Turned OFF	✓	✓	✓	✓
Wireless Devices					
Output name	ControllX	✓			✓
Type	Depends on the connected wireless device model				✓
Status	Turned OFF	✓	✓	✓	✓

MS Settings

Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
Management					
MS mode	Disabled	✓	✓	✓	✓
Account	9999		✓	✓	✓
GSM & SMS – attempts	5		✓	✓	✓
GSM & SMS – tel. number 1... 3	N/A		✓	✓	✓
PSTN – treat PSTN call as user call	Disable				✓
PSTN – attempts	5		✓	✓	✓
PSTN – tel. number 1... 3	N/A		✓	✓	✓
CSD – attempts	5		✓	✓	✓
CSD – tel. number 1... 5	N/A		✓	✓	✓
IP – IP attempts	3		✓	✓	✓

IP – test period	180 seconds		✓	✓	✓
IP – protocol	UDP	✓	✓	✓	✓
IP – unit ID	0000		✓	✓	✓
IP – communication protocol	EGR100		✓	✓	✓
IP – server IP	0.0.0.0	✓	✓	✓	✓
IP – server port	20000	✓	✓	✓	✓
Communication - primary	GPRS network		✓	✓	✓
Communication – backup 1… 5	N/A		✓	✓	✓
Delay after last communication attempt	600 seconds		✓	✓	✓
SIA IP protocol settings - encryption	Disabled				✓
SIA IP protocol settings – encryption key	0000				✓
SIA IP protocol settings – account prefix	N/A				✓
SIA IP protocol settings – receiver number	N/A				✓
SIA IP protocol settings – Contact ID ping	Disabled				✓
SIA IP protocol settings – data message	Event: 1602, partition: 01, user/zone: 000				✓
Data Messages					
Burglary alarm/restore – code	130				✓
Burglary alarm/restore – status	Enabled		✓	✓	✓
Main power loss/restore – code	301				✓
Main power loss/restore – status	Enabled		✓	✓	✓
Armed/disarmed by user – code	401				✓
Armed/disarmed by user – status	Enabled		✓	✓	✓
Test event – code	602				✓
Test event – status	Enabled		✓	✓	✓
Battery failed – code	309				✓
Battery failed – status	Enabled		✓	✓	✓
Battery dead or missing – code	311				✓
Battery dead or missing – status	Enabled		✓	✓	✓
Tamper alarm/restore – code	144				✓
Tamper alarm/restore – status	Enabled		✓	✓	✓
Silent zone alarm/restore – code	146				✓
Silent zone alarm/restore – status	Enabled		✓	✓	✓
Kronos ping – code	602				✓
Kronos ping – status	Enabled		✓	✓	✓
System started – code	900				✓
System started – status	Enabled		✓	✓	✓
24H zone alarm/restore – code	133				✓
24H zone alarm/restore – status	Enabled		✓	✓	✓
Fire zone alarm/restore – code	110				✓
Fire zone alarm/restore – status	Enabled		✓	✓	✓
Low battery – code	302				✓
Low battery – status	Enabled		✓	✓	✓
Temperature exceeded – code	158				✓
Temperature exceeded – status	Enabled		✓	✓	✓
Temperature fallen – code	159				✓
Temperature fallen – status	Enabled		✓	✓	✓
Wireless signal loss/restore – code	381				✓
Wireless signal loss/restore – status	Enabled		✓	✓	✓
Disarmed by user (duress code) – code	121				✓
Disarmed by user (duress code) – status	Enabled		✓	✓	✓
Armed/disarmed by user (SGS code) – code	463				✓
Armed by user (SGS code) – status	Enabled		✓	✓	✓
Armed/disarmed in STAY mode – code	456				✓
Armed/disarmed in STAY mode – status	Enabled		✓	✓	✓
Siren fail/restore – code	321				✓
Siren fail/restore – status	Disabled		✓	✓	✓
Date/time not set – code	626				✓
Date/time not set – status	Enabled		✓	✓	✓
GSM connection failed – code	358				✓
GSM connection failed – status	Enabled		✓	✓	✓
GSM antenna fail/restore – code	359				✓

GSM antenna fail/restore – status	Disabled		✓	✓	✓
System shutdown – code	414				✓
System shutdown – status	Enabled		✓	✓	✓
Keypad fail/restore – code	330				✓
Keypad fail/restore – status	Enabled		✓	✓	✓
GPRS connection lost – code	354				✓
GPRS connection lost – status	Enabled		✓	✓	✓
Zone bypass – code	570				✓
Zone bypass – status	Enabled		✓	✓	✓

Control / Scheduler					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
PGM output control 1... 16	Disabled				✓
Scheduler 1... 16	Disabled				✓
Additional conditions	Disabled				✓

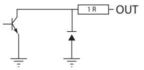
Peripheral Devices					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
Keypads					
Keypad 1... 4 partition	Partition 1		✓	✓	✓
Show armed status in keypad	Disabled				✓
Keypad partition switch	Disabled		✓	✓	✓
EKB3 mode	2 partitions				✓
Wireless keypads - partition	Partition 1		✓	✓	✓
Wireless keypads – backlight timeout	10 seconds				✓
Wireless keypads – bell	Disabled				✓
Siren					
EWS2 LED	Enabled		✓	✓	✓
Bell squawk	Disabled		✓	✓	✓
Activate siren if wireless device is lost	Disabled		✓	✓	✓
EWS3 fire alarm LED	Disabled		✓	✓	✓
EWS3 alarm LED	Disabled		✓	✓	✓
Bell squawk enabled if arming in STAY mode	Disabled		✓	✓	✓
Temperature Sensors					
Temperature sensor 1... 8 name	N/A	✓			✓
Temperature sensor 1... 8 min. temperature	0	✓	✓	✓	✓
Temperature sensor 1... 8 max. temperature	0	✓	✓	✓	✓
Primary	No.1	✓	✓	✓	✓
Secondary	No.2	✓	✓	✓	✓
iButton Keys					
iButton key name	N/A				✓
iButton key partition	Partition 1		✓	✓	✓
Allow adding new iButton keys	Disabled	✓	✓	✓	✓

System					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
Management					
Mains power loss delay	30 seconds		✓	✓	✓
Mains power restore delay	120 seconds		✓	✓	✓
Alarm duration	1 minute	✓	✓	✓	✓
Wireless channel	Depends on firmware				✓
Periodic test	Every 1 day at 11:00	✓	✓	✓	✓
Microphone level	12		✓		✓
Speaker level	85		✓		✓

Service mode	Disabled	✓	✓	✓	✓
Smart Security					
Smart Security	Disabled				✓
Server address	ss.eldes.lt				✓
Port	8082				✓
Ping period	180 seconds				✓
Time zone	N/A				✓
Communication	Via GPRS network				✓
GPRS Settings					
SIM1... SIM2 APN	N/A	✓			✓
SIM1... SIM2 user name	N/A	✓			✓
SIM1... SIM2 password	N/A	✓			✓
DNS1	N/A	✓	✓	✓	✓
DNS2	N/A	✓	✓	✓	✓

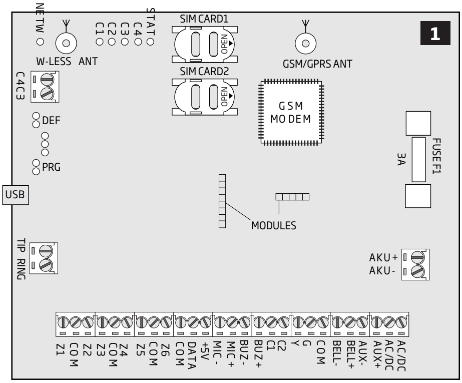
2. TECHNICAL SPECIFICATIONS

2.1. Electrical & Mechanical Characteristics

Electrical & Mechanical Characteristics	
Main power supply	16-24V 50 Hz ~1.5A max / 18-24V ⎓ 1,5A max
Current in standby without external sensors and keypad	Up to 80mA
Recommended backup battery voltage, capacity	12V; 1,3-7 Ah
Recommended backup battery type	Lead-Acid
Backup battery charge current	Up to 500mA
Backup battery charge duration	Up to 30 hours for 7Ah battery
Gsm modem frequency	850/900/1800/1900MHz
Cable type for GSM/GPRS antenna connection	Shielded
Number of zones on-board	6 (ATZ mode: 12)
Nominal zone resistance	5,6kΩ (ATZ Mode: 5,6kΩ and 3,3kΩ)
Number of PGM outputs on-board	4
On-board PGM output circuit	 Open Collector Output. Output is pulled to COM when turned ON.
Maximum commuting on-board PGM output values	4 x Voltage – 30V; current – 500mA.
BELL: Siren output when activated	Connected to COM
BELL: Maximum siren output current	1A
BELL: Maximum cable length for siren connection	Up to 100 meters
BELL: Cable type for siren connection	Unshielded
AUX: Auxiliary equipment power supply voltage	13,8V DC
AUX: Maximum accumulative current of auxiliary equipment	1,1A
AUX: Maximum cable length for auxiliary equipment connection	Up to 100 meters
AUX: Cable type for auxiliary equipment connection	Unshielded
BUZ: Maximum current of mini buzzer	150mA
BUZ: Power supply voltage of buzzer	5V DC
BUZ: Cable type for mini buzzer connection	Unshielded
Supported temperature sensor model	Maxim®/Dallas® DS18S20, DS18B20
Maximum supported number of temperature sensors	8
DATA: Maximum cable length for 1-Wire communication	Up to 30 meters
DATA: Cable type for 1-Wire communication	Unshielded
Supported iButton key model	Maxim®/Dallas® DS1990A
Maximum supported number of iButton keys	16
Maximum supported number of keypads	4 x EKB2 / EKB3
Y/G: Maximum cable length for RS485 communication	Up to 100 meters
Y/G: Cable type for RS485 communication	Unshielded
MIC: Maximum cable length for microphone connection	Up to 2 meters
MIC: Cable type for microphone connection	Unshielded
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Wireless communication range	Up to 30m in premises; up to 150m in open areas
Maximum supported number of wireless devices	32
Event log size	500 events
Maximum supported number of zones	76
Maximum supported number of PGM outputs	76
Cable type for zone and PGM output connection	Unshielded
Communications	SMS, Voice calls, GPRS network, RS485, CSD, PSTN, Ethernet via ELAN3-ALARM
Supported protocols	Ademco Contact ID, EGR100, Kronos, Cortex SMS, SIA IP
Dimensions	140x100x18mm
Operating temperature range	-20...+55 °C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)

2.2. Main Unit, LED & Connector Functionality

Main Unit Functionality	
GSM MODEM	GSM network 850/900/1800/1900MHz modem
SIM CARD1	Primary SIM card slot / holder
SIM CARD2	Secondary SIM card slot / holder
DEF	Pins for restoring default settings
USB	Mini USB port
FUSE F1	3A fuse
W-LESS ANT	Wireless antenna SMA type connector
GSM/GPRS ANT	GSM/GPRS antenna SMA type connector
MODULES*	Slots for EA1, EA2 or EPGM8 module



LED Functionality	
NETW	GSM network signal strength
C1	PGM output C1 status - ON/OFF
C2	PGM output C2 status - ON/OFF
C3	PGM output C3 status - ON/OFF
C4	PGM output C4 status - ON/OFF
STAT	Micro-controller status

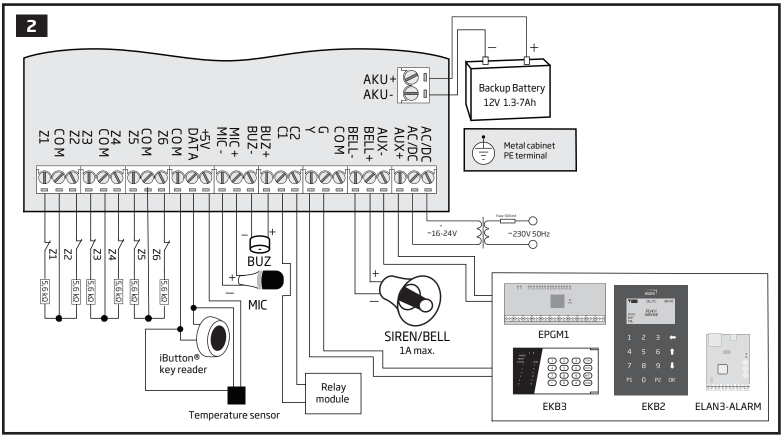
NETW indication	GSM signal strength
OFF	No GSM signal
Flashing every 3 sec.	Poor
Flashing every 1 sec.	Medium
Flashing several times per sec.	Good
Steady ON	Excellent

Connector Functionality	
TIP*	PSTN (landline) terminal
RING*	PSTN (landline) terminal
DATA	1-Wire interface for iButton key & temperature sensor connection
+5V	Temperature sensor power supply terminal (+5V)
MIC-	Microphone negative terminal
MIC+	Microphone positive terminal
BUZ-	Buzzer negative terminal
BUZ+	Buzzer positive terminal
C1 - C4	PGM output terminals
Z1 - Z6	Security zone terminals
Y	RS485 interface CLOCK terminal (yellow wire)
G	RS485 interface DATA terminal (green wire)
COM	Common return terminal
BELL-	Siren negative terminal
BELL+	Siren positive terminal
AUX-	Negative power supply terminal for auxiliary equipment
AUX+	Positive power supply terminal for auxiliary equipment
AC/DC	Main power supply terminals
AKU-	Backup battery negative terminal
AKU+	Backup battery positive terminal

* - Optional, implementable on request in advance

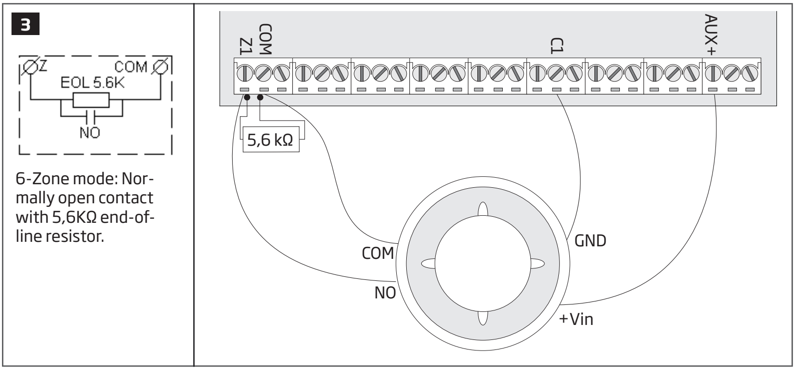
2.3. Wiring Diagrams

2.3.1.General Wiring



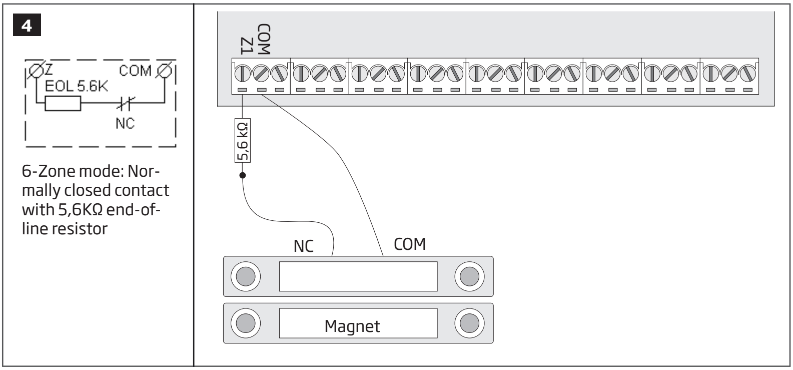
2.3.2. Zone Connection Types

Type 1 Example of 4-wire smoke detector wiring



6-Zone mode: Normally open contact with 5,6KΩ end-of-line resistor.

Type 2 Example of magnetic door contact wiring



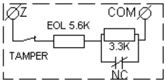
6-Zone mode: Normally closed contact with 5,6KΩ end-of-line resistor

NOTE: Based on the example given, in the event of an alarm, the smoke detector could be reset by turining OFF and ON the PGM output C1. For more details, please refer to **18.4. Turning PGM Outputs ON and OFF.**

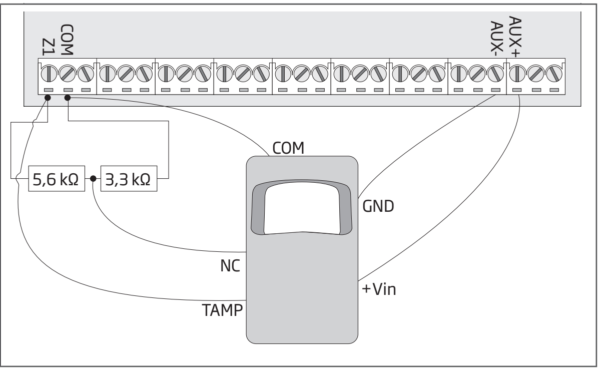
NOTE: The system does NOT support 2-wire smoke detectors.

Type 3 Example of motion detector wiring

5

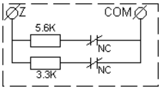


6-Zone mode: Tamper and 5,6KΩ end-of-line resistor and 3,3KΩ end-of-line resistor with normally closed contact.

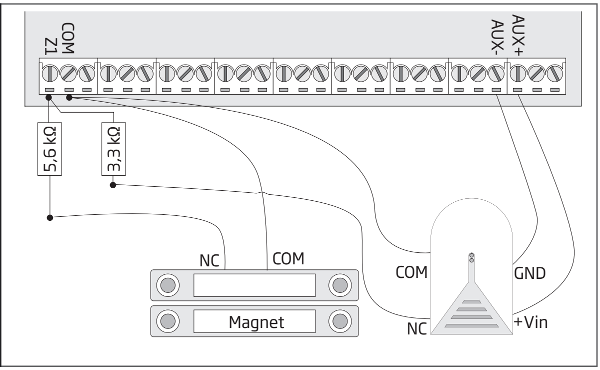


Type 4 Example of magnetic door contact (Z1) and glass break sensor (Z7) wiring

6

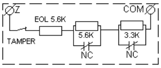


ATZ mode: 5,6KΩ end-of-line resistor and normally closed contact with 3,3KΩ end-of-line resistor and normally closed contact

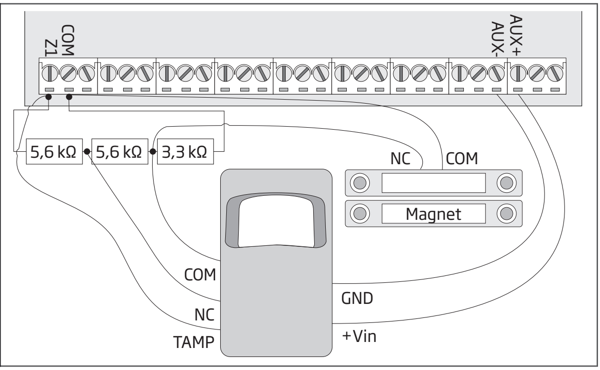


Type 5 Example of motion detector (Z1) and magnetic door contact (Z7) wiring

7

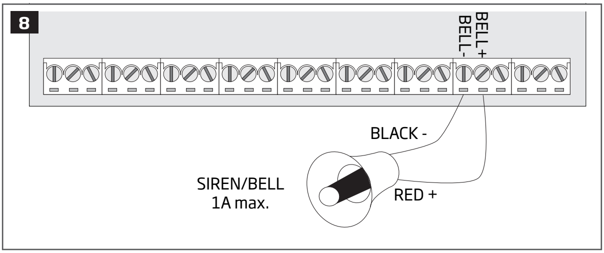


ATZ mode: Tamper, 5,6KΩ end-of-line resistor, 5,6KΩ end-of-line resistor with normally closed contact and 3,3KΩ end-of-line resistor with normally closed contact.



See also **14.3. 6-Zone Mode** and **14.4. ATZ (Advanced Technology Zone) Mode.**

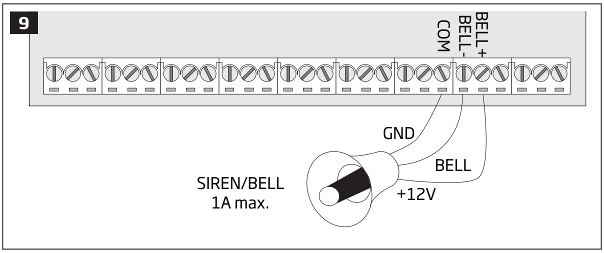
2.3.3. Siren



Piezo siren

1 Connect positive siren wire (red) to **BELL+** terminal.

2 Connect negative siren wire (black) to **BELL-** terminal.

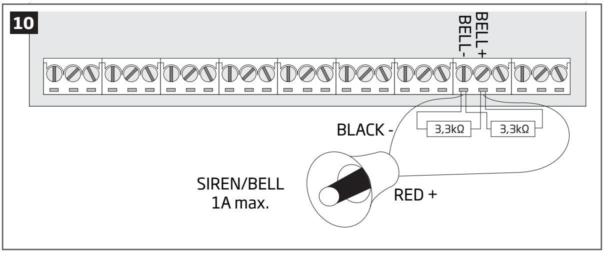


Self-contained siren

1 Connect negative **GND** siren wire to **COM** terminal.

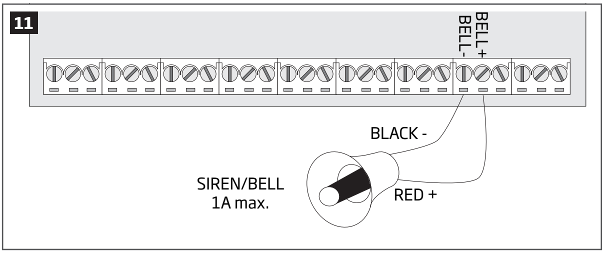
2 Controlling **BELL** siren wire must be connected to **BELL-** terminal.

3 Connect positive **+12V** siren wire to **BELL+** terminal.



Siren status monitoring

By default, the system monitors siren status and indicates system fault on the keypad if the siren is broken/disconnected. However, this feature requires a pair of parallelly connected resistors of 3,3kΩ nominal across **BELL+** and **BELL-** terminals.



No siren status monitoring

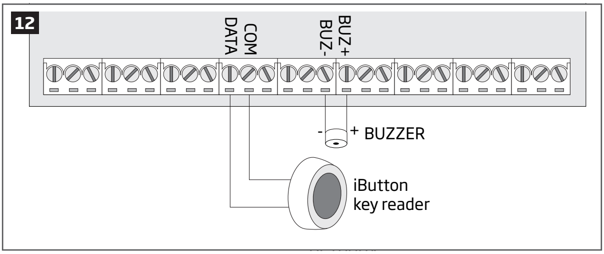
If the siren status monitoring feature is not required, do not connect any resistor in parallel and disable siren fault indication on the keypad (see **29. INDICATION OF SYSTEM FAULTS**).

See also **20. SIREN/BELL**.

NOTE: BELL- is the commuted terminal intended for siren control.

NOTE: Siren status monitoring feature supervises the resistance across **BELL+** and **BELL-** terminals. The resistance must be ranging from 1kΩ through 3,3kΩ, otherwise the system will indicate system fault. In order to view the siren resistance value, please refer to Diagnostic Management feature available on *ELDES Configuration Tool* software.

2.3.4. iButton Key Reader and Buzzer



Supported iButton key model: Maxim/Dallas DS1990A

The iButton key reader can be installed with buzzer or separately. The buzzer is intended for audio indication of exit/entry delay countdown providing short beeps.

1 Connect iButton key reader terminal wires to 1-Wire interface: **COM** and **DATA** terminals respectively.
2 Connect buzzer's negative terminal wire to **BUZ-** and positive terminal wire to **BUZ+.**
3 Additionally, a LED indicator for visual indication can be installed in parallel to buzzer or instead. Connect LED anode terminal to **BUZ-** and cathode to **BUZ+**.

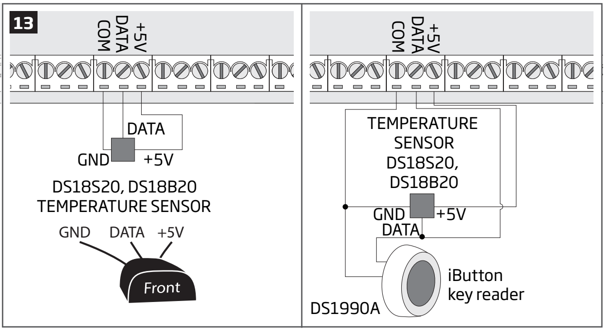
NOTE: The installation of buzzer is not necessary if EKB2/EKB3 keypad is used.

ATENTION: The cable length for connection to 1-Wire interface can be up to 30 meters max.

2.3.5. Temperature Sensor and iButton Key Reader

Supported iButton key model: Maxim/Dallas DS1990A

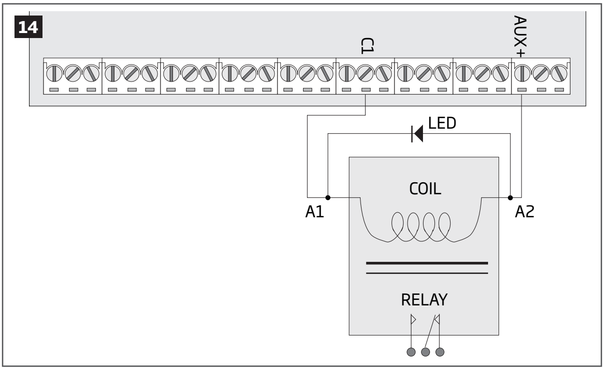
Supported temperature sensor model: Maxim/Dallas DS18S20, DS18B20



1 Connect temperature sensor **GND**, **DATA**, **+5V** terminals to 1-Wire interface: **COM**, **DATA** and **+5V** terminals respectively.
2 When connecting iButton key reader in parallel to temperature sensor, connect iButton key reader terminal wires to **COM** and **DATA** terminals respectively.

ATENTION: The cable length for connection to 1-Wire interface can be up to 30 meters max.

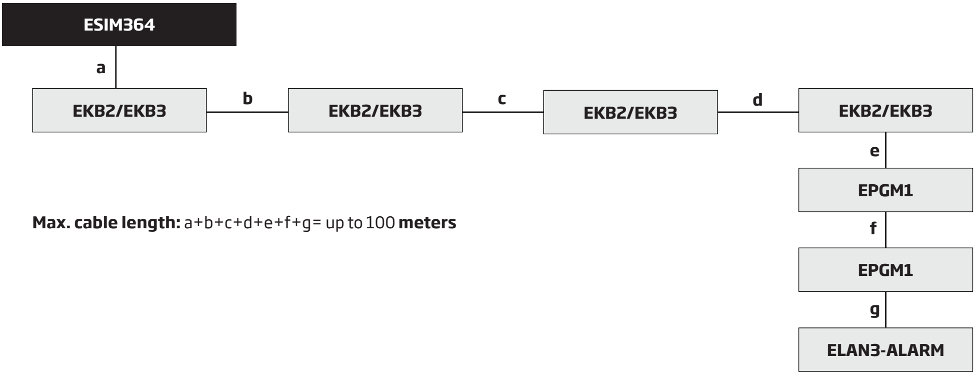
2.3.6. Relay Finder 40.61.9.12 with Terminal Socket 95.85.3 to PGM Output



1 Wire up relay **A1** terminal to **PGM** output **Cx** and **A2** terminal to **AUX+**.
2 In addition, connect LED indicator's anode terminal to relay **A2** terminal and cathode to **A1** terminal.

2.3.7. RS485

Serial Wiring Method



Max. cable length: a+b+c+d+e+f+g= up to 100 **meters**

NOTE: If necessary, the RS485 devices can be powered from an external 12-14V DC power supply instead of AUX+ and AUX- terminals

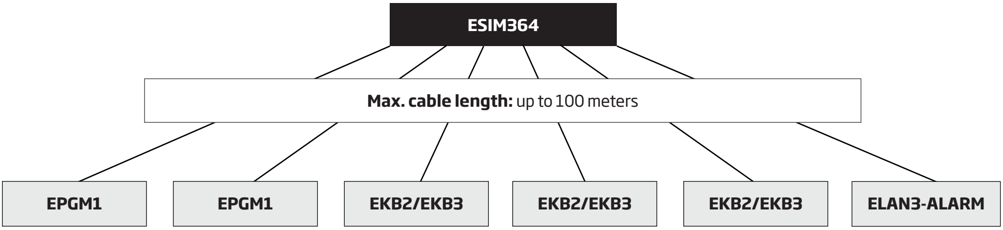
ATTENTION: The cable length must not exceed 100 meters in total.

ATTENTION: When wiring more than 1 keypad and/or EPGM1 module, please ensure that the set address of each keypad and/or EPGM1 module is different.

NOTE: You may connect only 1 EKB2/EKB3 keypad or a mixed combination of EKB2 and EKB3 keypads. The combination can consist of up to 4 keypads in total.

For more details on RS485 device installation, please refer to **32.1. RS485 Interface**

Parallel Wiring Method



NOTE: If necessary, the RS485 devices can be powered from an external 12-14V DC power supply instead of AUX+ and AUX- terminals

ATTENTION: The cable between ESIM364 and each RS485 device must be of the same length and can NOT exceed 100 meters.

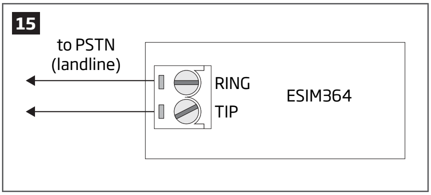
ATTENTION: When wiring more than 1 keypad and/or EPGM1 module, please ensure that the set address of each keypad and/or EPGM1 module is different.

NOTE: You may connect only 1 EKB2/EKB3 keypad or a mixed combination of EKB2 and EKB3 keypads. The combination can consist of up to 4 keypads in total.

For more details on RS485 device installation, please refer to **32.1. RS485 Interface**

2.3.8. RING/TIP

15



ATTENTION: The **TIP/RING** connectors and PSTN module are NOT included in a standard ESIM364 alarm system unit. These components are optional and can be implemented on request in advance.

3. INSTALLATION

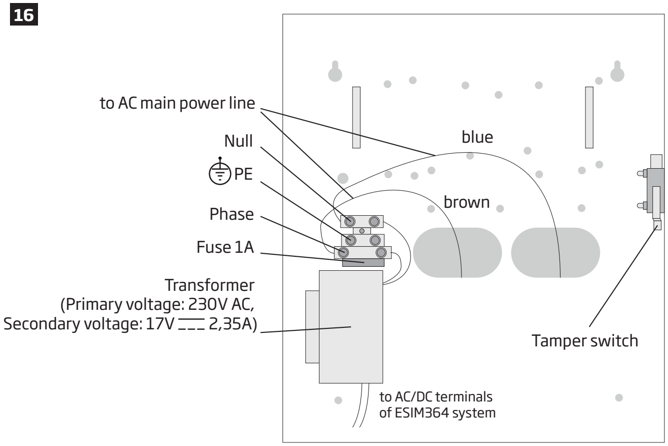
When professional installation, OEM integration or assembly by a third-party is expected, the installation instructions and assembly requirements approved for equipment approval must be provided to the integrators to clearly identify the specific requirements necessary to maintain RF exposure compliance. The grantee of a transmitter, typically the manufacturer, is responsible for ensuring installers and integrators have a clear understanding of the compliance requirements by including the required instructions and documentation with the product and, if necessary, to provide further support to fulfill grantee responsibilities for ensuring compliance. The integrators must be fully informed of their obligations and verify the resolution of any issues and concerns with each transmitter manufacturer or grantee.

- The system can be installed in a metal or non-flammable cabinet only. For a convenient installation, ME1 metal cabinet is highly recommended. When using a different metal cabinet, it is necessary to ground it.
- For the connection of 230V transformer, use 3x0.75 mm^2 1 thread double isolated cable. 230V power supply cables must not be grouped with low voltage cable group.
- For the connection of auxiliary and BELL outputs, use 2x0.75 mm^2 1 thread unshielded cable of up to 100 meters length.
- For the connection of zone/PGM output connectors, use 0.50 mm^2 1 thread unshielded cable of up to 100 meters length.

System Installation in ME1 Metal Cabinet

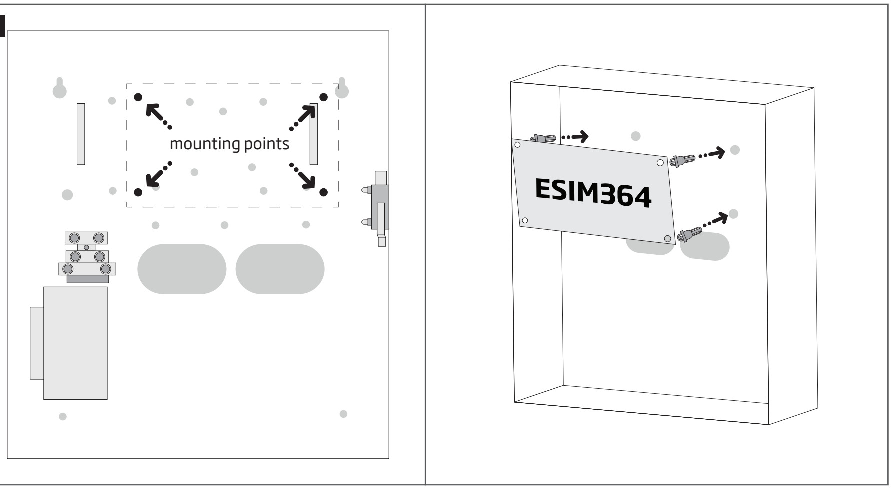
1. ME1 metal cabinet components

16

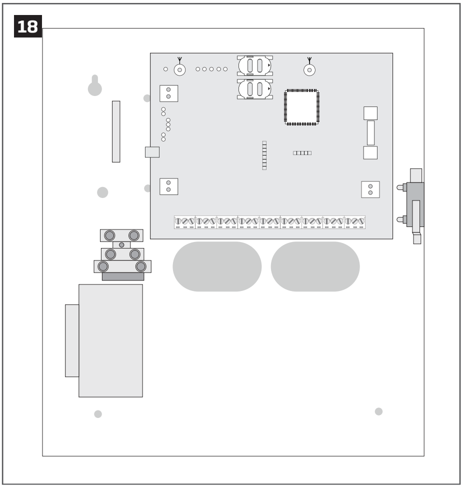


2. Insert the plastic standoffs into the appropriate mounting points and fix the board of ESIM364 on the holders as indicated below.

17

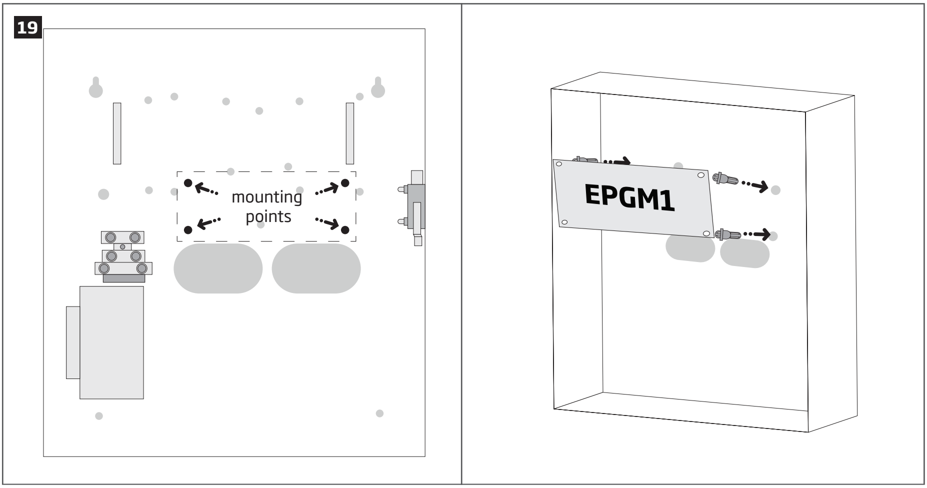


18

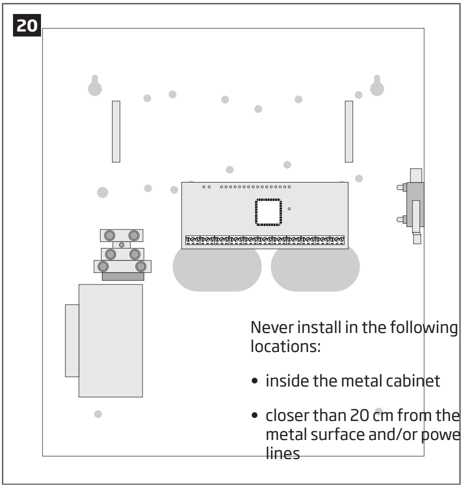


3. If EPGM1 module is to be installed, please install it in the first place and ESIM364 alarm system afterwards. EPGM1 must be mounted on the shorter plastic standoffs, while ESIM364 – on the longer ones. The mounting points of EPGM1 module are indicated below.

19



Inserting a SIM card into SIM CARD1 slot is mandatory as it is the main SIM card slot, while using a SIM card in SIM CARD2 slot is optional.

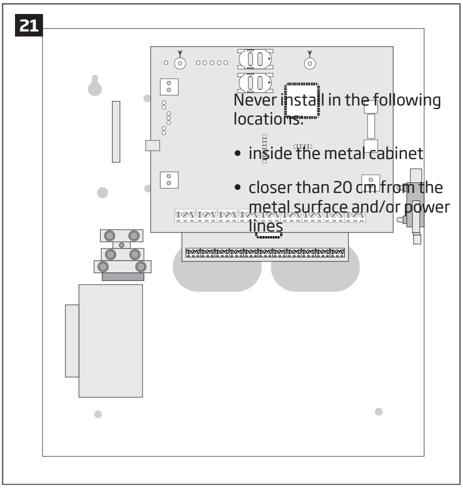


Never install in the following locations:

- inside the metal cabinet
- closer than 20 cm from the metal surface and/or power lines

Recommended installation:

- keep the distance of at least 20 cm or more.



Never install in the following locations:

- inside the metal cabinet
- closer than 20 cm from the metal surface and/or power lines

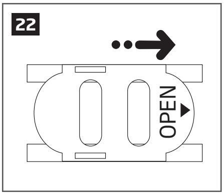
Recommended installation:

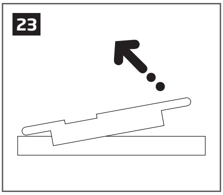
- face the front side of the wireless device towards the antenna
- keep the distance: 0.5 m to 30 m inside the building, 0.5 m to 150 m in open areas

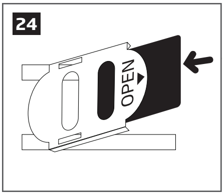
4. Wire up the system according to the wiring diagrams. Install the buzzer closer to iButton key reader in order to hear the exit delay countdown. A LED indicator can be used in parallel to the buzzer or instead. For a convenient installation, ED1 is highly recommended (see **2.3 Wiring Diagrams** for more details).

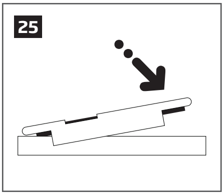
5. Disable the PIN code of the SIM card by inserting it into a mobile phone and following the proper menu steps. Ensure that the additional services, such as **voice mail, call forwarding, report on missed/busy calls ("call catcher")** are disabled on the SIM card. For more details on how to disable these services, please contact your GSM operator.

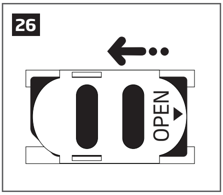
6. Once the PIN code is disabled, place the SIM card into the SIM CARD1 slot of the alarm system. If Dual-SIM feature is to be used, insert another SIM card into the SIM CARD2 slot. For more details, please refer to **31. DUAL-SIM MANAGEMENT.**



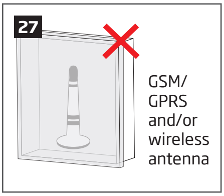


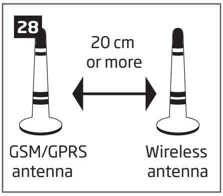




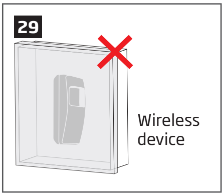


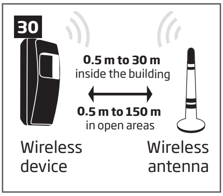
7. Connect the GSM/GPRS and wireless antennas and follow the recommendations for the installation:





8. If one or more wireless devices are to be bound, follow the recommendations for the installation to achieve the strongest wireless signal:





For more details on how to install the wireless devices, please refer to **33. ELDES WIRELESS DEVICES** and **RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION** manual located at www.eldes.lt/download

9. Power up the system and wait until indicator STAT lights up.

10. The system starts up in less than a minute. Indicator STAT should be flashing indicating successful micro-controller operation.

11. The illuminated indicator NETW indicates that the system successfully registered to GSM network. To find the strongest GSM signal, place the GSM/GPRS antenna and follow the indications provided by NETW indicator (see **2.3. Main Unit, LED & Connector Functionality**).

12. Change the default SMS password (see **6. SMS PASSWORD AND INSTALLER CODE** for more details).

13. Set the phone number for User 1 (see **8. USER PHONE NUMBERS** for more details).

14. Set system date and time (see **9. DATE AND TIME** for more details).

15. Once the system is fully configured, it is ready for use. However, if you fail to receive an SMS reply from the system, please check the SMSC (Short Message Service Center) phone number. For more details regarding the SMS centre phone number, please refer to **27.1. SMSC (Short Message Service Center) Phone Number.**

16. If it is required to change the batteries for the wireless devices or carry out other system maintenance tasks, please activate the Service mode. For more detail regarding this mode, please refer to **34. SERVICE MODE.**

ATTENTION: The system is NOT compatible with pure 3G SIM cards. Only 2G/GSM SIM cards and 3G SIM cards with 2G/GSM profile enabled are supported. For more details, please contact your GSM operator.

NOTE: The installation of iButton key reader, EKB2/EKB3/EKB3W keypad, EWK1 wireless keyfob is not mandatory. However, it is recommended to have those devices installed as an emergency switch in case your mobile phone is switched off or missing.

NOTE: We advise you to choose the same GSM SIM provider for your system as for your mobile phone. This will ensure the fastest, most reliable SMS text message delivery service and phone call connection.

NOTE: Even though alarm system ESIM364 installation process is not too complicated, we still recommend to perform it by a person with basic knowledge in electrical engineering and electronics to avoid any system damage.

4. GENERAL OPERATIONAL DESCRIPTION

When the system is being armed, it will initiate the exit delay countdown intended for the user to leave the secured area. During the countdown period the buzzer will emit short beeps. By default, exit delay duration is 15 seconds. After the countdown is complete, the system will become armed and lock the configuration by keypad possibility. In case the user does not leave the secured area before the countdown is complete, the system will will arm in Stay mode if at least 1 zone has Stay attribute enabled. By default, if there is at least 1 violated zone or tamper, the user will not be able to arm the system until the violated zone or tamper is restored. In case it is required to arm the alarm system despite the violated zone presence, the violated zone can be bypassed or Force attribute enabled.

After the system is armed and if a zone (depending on type) or tamper is violated, the system will cause an alarm lasting for 1 minute (by default), During the alarm, the siren/bell will provide an alarm sound along with the buzzers of the keypads. By default, the system will also makes a phone call and send an SMS text message containing the violated zone or tamper number to a preset user and indicate the violated zone or tamper number on the keypad. If another zone or tamper is violated or the same one is restored and violated again during the alarm, the system will act as mentioned previously, but will not extend the alarm time.

After the user enters the secured area, the system will initiate the entry delay countdown intended for system disarming. During the countdown period, the buzzer will emit a steady beep. By default, entry delay duration is 15 seconds. After the user successfully performs the disarming process, the system will unlock the keypads. If the user does not disarm the system in time, the alarm system will cause an instant alarm.

NOTE: The alarm will be caused even if a tamper is violated while the system is disarmed.

For more details, please refer to **12. ARMING AND DISARMING**.

5. CONFIGURATION METHODS

!

!!! In this installation manual the underscore character "_" represents one space character. Every underscore character must be replaced by a single space character. There must be no spaces or other unnecessary characters at the beginning and at the end of the SMS text message.

EN50131-1 **GRADE 3**

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All codes and passwords must consist of 6 digits.
- The system must prompt for master (see **10. MASTER AND USER CODES**) and installer (see **6. SMS PASSWORD AND INSTALLER CODE**) codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool* software.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **36. EN 50131-1 GRADE 3**

5.1. SMS Text Messages

SMS

In order to configure and control the system by SMS text message, send the text command to the ESIM364 system phone number from one of the preset user phone numbers. The structure of SMS text message consists of 4-digit SMS password (the default SMS password is 0000 – four zeros), the parameter and value. For some parameters the value does not apply e. g. STATUS. The variables are indicated in lower-case letters, while a valid parameter value range is indicated in brackets.

5.2. EKB2 LCD Keypad

EKB2

The system configuration and control by EKB2 keypad is carried out by navigating throughout the menu section list displayed on LCD screen. To navigate in the menu path, touch ↓, ↑ keys to select the desired menu section and touch OK key to open the selected section. To enter a required value, use 0... 9 keys and touch OK key for confirmation or cancel/go one menu section back by touching ← key. The value can be typed in directly by touching 0... 9 keys while highlighting the desired menu section. EKB2 menu type is "circle", therefore when the last section in the menu list is selected, you will be brought back to the beginning of the list after touching the ↓ key. In this installation manual, the menu path is based on the EKB2 menu tree by starting at home screen view (see **32.1.1.6. EKB2 Menu Tree**). The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

NOTE: By default, menu section CONFIGURATION is secured with installer code. The default installer code is 1470.

NOTE: The system can be configured using only one keypad at a time. Other connected keypads will be inactive while the menu section CONFIGURATION is opened. The inactive EKB2 keypads will display 🛠 icon.

NOTE: The keypad will automatically exit the menu section CONFIGURATION and return to home screen view if 1 minute after the last key-touch expires.

5.3. EKB3/EKB3W LED Keypad

EKB3/ EKB3W

The system configuration and control by EKB3/EKB3W keypad is carried out by activating the Configuration mode using the installer code (by default – installer code is 1470) and entering a valid configuration command using the number keys [0]... [9], [#] key for confirmation and [*] key to clear the characters that have been entered. Alternatively, the user can wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the entered characters have been cleared. When typing in the characters, the indication of each pressed key is provided by short beep of keypad buzzer and red indicators when the number keys [0]... [9] are being pressed. Some commands require [STAY], [BYPS], [INST] and [CODE] keys as well. The structure of a standard configuration command is a combination of digits. The commands, which do not require the Configuration mode being activated, are noted. The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

NOTE: If you have accidentally typed in an unnecessary character (-s), please press [*] key or wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the typed in characters have been cleared.

NOTE for EKB3W: Even if Back-light Timeout has expired, the character will be considered as type in once the appropriate EKB3W key is pressed. For more details, please refer to **33.1.7. Wireless Communication, Sleep Mode and Back-light Timeout .**

Activate/deactivate Configuration mode

EKB3/ EKB3W

Enter installer code:
[INST] iiii #
Value: *iiii*– 4-digit installer code.
Example: *INST1470#*

EN50131-1 **GRADE 3**

Activate/deactivate Configuration mode

EKB3/ EKB3W

Enter installerr and master codes:
[INST] iiiiii mmmmmm #
Value: *iiiiii* – 6-digit installer code; *mmmmmm* - 6-digit master code.
Example: *INST147000111111#*

Deactivate Configuration mode

EKB3/ EKB3W

Enter installerr code:
[INST] iiiiii #
Value: *iiiiii* – 6-digit installer code.
Example: *INST147000#*

The following table provides a list of EKB3/EKB3W indications, which are relevant during Configuration mode.

Indication	Description
Indicator ARMED flashing	Configuration mode activated successfully.
Indicator SYSTEM flashing	Valid parameter is entered and waiting for valid value to be enetered.
1 long beep	Non-existing command or invalid parameter value entered.
3 short beeps	Command entered successfully.

NOTE: The system can be configured using only one keypad at a time. Other connected keypads will be inactive while the Configuration mode is activated.

NOTE: Configuration mode will automatically deactivate if 1 minute after the last key-stroke expires.

5.4. ELDES Configuration Tool Software

Config Tool

Software *ELDES Configuration Tool* is intended for ESIM364 alarm system configuration locally via USB port or remotely via GPRS network or Ethernet connection (ELAN3-ALARM device required). This software simplifies system configuration process by allowing to use a personal computer in the process. Before starting to use *ELDES Configuration Tool* software, please read the user guide provided in the software's HELP section.

5.4.1. Remote System Configuration via Configuration Server

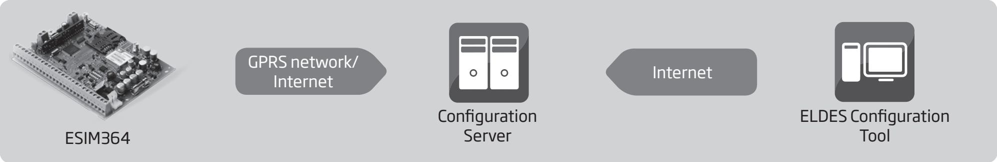
ATTENTION: The system will NOT send any data to monitoring station while configuring the system remotely via GPRS network or Ethernet connection. However, during the configuration session, the data messages are queued up and transmitted to the monitoring station after the configuration session is over.

ATTENTION: When the Configuration mode is activated by EKB3/EKB3W keypad or menu section CONFIGURATION is opened by the installer using EKB2 keypad, remote system configuration will be disabled.

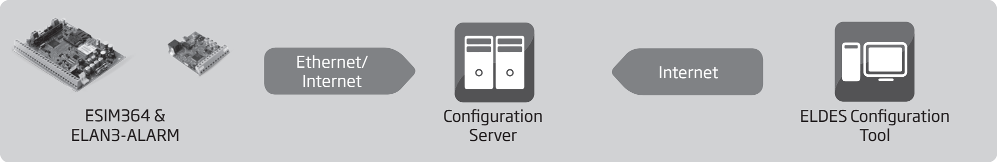
NOTE: The keypads will be inactive when the system is being configured remotely.

Before configuring ESIM364 remotely using GPRS network or Ethernet (using ELAN3-ALARM) connection, please ensure that:

- SIM card is inserted into SIM CARD1 slot of ESIM364 device (see **2.2. Main Unit, LED & Connector Functionality**).
- Mobile internet service (GPRS) is enabled on the SIM card – required for GPRS network connection only.
- APN, user name and password are set up (see **30.2.1. GPRS Network**) – required for GPRS network connection only.
- Power supply is connected to ESIM364.
- Default SMS password is changed to a new 4-digit password (see **6. SMS PASSWORD AND INSTALLER CODE**).
- At least User 1 phone number is set up (see **8. USER PHONE NUMBERS**).



Remote system configuration via GPRS network connection



Remote system configuration via Ethernet connection using ELAN3-ALARM

a) In order to activate a remote connection between ESIM364 system and ELDES configuration server, please send the following SMS text message from preset user phone number. Upon the successful SMS text message delivery, the system establishes a connection session for 20 minutes.

Initiate connection with ELDES server

GPRS

SMS text message content:
ssss_STCONFIG
Value: *ssss* – 4-digit SMS password.
Example: *1111_STCONFIG*

ELAN3 ALARM

SMS text message content:
ssss_STCONFIG:ELAN
Value: *ssss* – 4-digit SMS password.
Example: *1111_STCONFIG:ELAN*

b) Once the SMS text message containing device IMEI number and confirming a successful connection establishment is received, please run *ELDES Configuration Tool* software.

c) Click **Remote Connection Management...**

d) In the next window, select **Connect to Remote Server (recommended)** and click **Next** button.

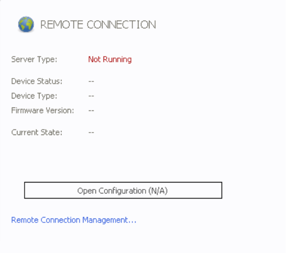
e) In **Device IMEI** entry, enter the IMEI number previously received by SMS text message.

f) Click **Continue** button.

g) By default, upon the successfully established connection, the system will prompt for an installer code.

h) By entering a valid installer code, the system grants access to full configuration remotely.

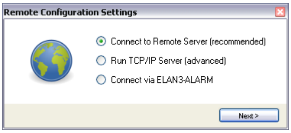
i) **Remote Configuration Management** window displays all performed configuration actions and connectivity information.


REMOTE CONNECTION

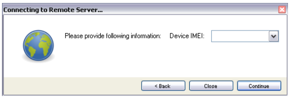
Server Type: Not Running

Device Status: --
Device Type: --
Firmware Version: --

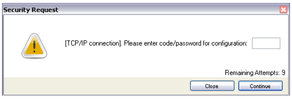
Current State: --


Remote Configuration Settings

● Connect to Remote Server (recommended)
○ Run TCP/IP Server (advanced)
○ Connect via ELAN3-ALARM

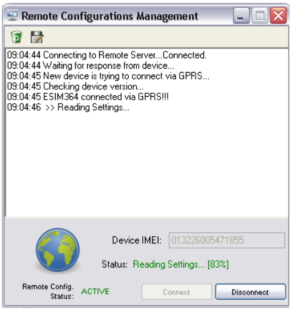

Connecting to Remote Server...

Please provide following information: Device IMEI:


Security Request

[TCP/IP connection]. Please enter code/password for configuration:

Remaining Attempts: 9


Remote Configurations Management

```
09:04:44 Connecting to Remote Server...Connected.
09:04:44 Waiting for response from device...
09:04:45 New device is trying to connect via GPRS...
09:04:45 Checking device version...
09:04:45 ESIM364 connected via GPRS!!!
09:04:46  >> Reading Settings...
```

Device IMEI: 013226005471855

Status: Reading Settings... [83%]

Remote Config. Status: ACTIVE

5.4.2. Remote System Configuration via Direct Connection

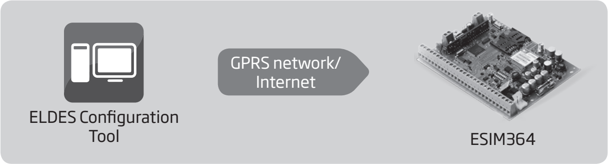
ATTENTION: The system will NOT send any data to monitoring station while configuring the system remotely via GPRS network or Ethernet connection. However, during the configuration session, the data messages are queued up and transmitted to the monitoring station after the configuration session is over.

ATTENTION: When the Configuration mode is activated by EKB3/EKB3W keypad or menu section CONFIGURATION is opened by the installer using EKB2 keypad, remote system configuration will be disabled.

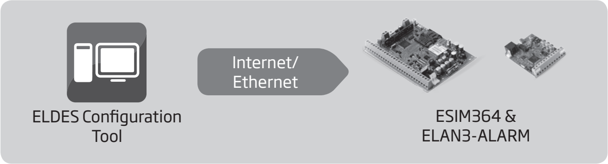
NOTE: The keypads will be inactive when the system is being configured remotely.

Before configuring ESIM364 remotely using GPRS network or Ethernet (using ELAN3-ALARM) connection, please ensure that:

- SIM card is inserted into SIM CARD1 slot of ESIM364 device (see **2.2. Main Unit, LED & Connector Functionality**) – required for GPRS network connection only.
- Mobile internet service (GPRS) is enabled on the SIM card – required for GPRS network connection only.
- APN, user name and password are set up (see **30.2.1. GPRS Network**) – required for GPRS network connection only.
- Machine running *ELDES Configuration Tool* software provides access via public IP address.
- TCP port 5000 is forwarded for the IP address of the machine running *ELDES Configuration Tool* software.
- Power supply is connected to ESIM364.



Remote system configuration via GPRS network connection



Remote system configuration via Ethernet connection

5.4.2.1. Establishing Remote Connection Between ESIM364 System and ELDES Configuration Tool via GPRS Network

GPRS

a) Run *ELDES Configuration Tool* software.

b) Click **Remote Connection Management...**

c) In the next window, select Run **TCP/IP Server (advanced)** and click Next button.

d) Set a TCP port for listening for incoming connections or leave the default TCP port 5000.

e) Click **Continue** button.

f) In order to activate a remote connection between ESIM364 system and *ELDES Configuration Tool* software running as remote configuration server, please send the following SMS text message from preset user phone number. Upon the successful SMS text message delivery, the system establishes a connection session for 20 minutes.

Initiate connection with ELDES Configuration Tool

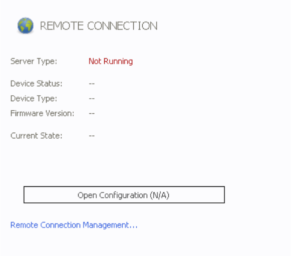
GPRS

SMS text message content:
ssss_STCONFIG:add.add.add.add:pprrt or
ssss_STCONFIG:host-name:pprrt
Value: *ssss* – 4-digit SMS password; add.add.add.add – public IP address of the machine running ELDES Configuration Tool software; *pprrt* – TCP port number, range – [1... 65535]; *host-name* – public host-name of the machine running *ELDES Configuration Tool* software.
Example: *1111_STCONFIG:62.80.115.102:4522*

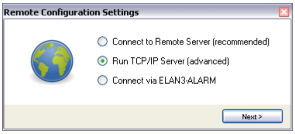
g) By default, upon the successfully established connection, the system will prompt for an installer code.

h) By entering a valid installer code, the system grants access to full configuration remotely.

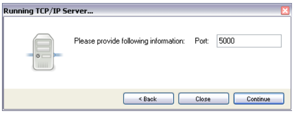
i) **Remote Configuration Management** window displays all performed configuration actions and connectivity information.


REMOTE CONNECTION

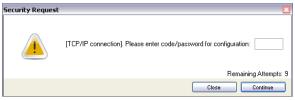
Server Type: Not Running
Device Status: --
Device Type: --
Firmware Version: --
Current State: --


Remote Configuration Settings

○ Connect to Remote Server (recommended)
● Run TCP/IP Server (advanced)
○ Connect via ELAN3-ALARM

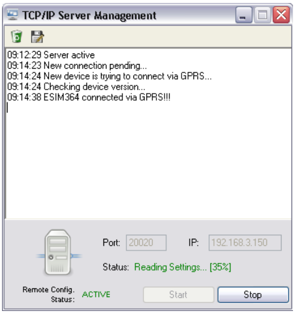

Running TCP/IP Server...

Please provide following information: Port: 5000


Security Request

[TCP/IP connection]. Please enter code/password for configuration:

Remaining Attempts: 9


TCP/IP Server Management

```
09:12:29 Server active
09:14:23 New connection pending...
09:14:24 New device is trying to connect via GPRS...
09:14:24 Checking device version...
09:14:38 ESIM364 connected via GPRS!!!
```

Port: 20020 IP: 192.168.3.150
Status: Reading Settings... [35%]
Remote Config. Status: ACTIVE

5.4.2.2. Establishing Remote Connection Between ESIM364 System and ELDES Configuration Tool via Ethernet Using ELAN3-ALARM

ELAN3 ALARM

a) Run *ELDES Configuration Tool* software.

b) Click **Remote Connection Management...**

c) In the next window, select **Connect** via ELAN3-ALARM and click **Next** button.

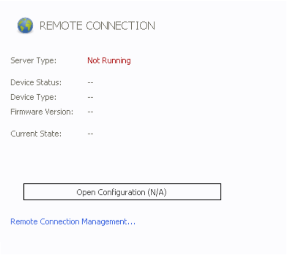
d) Click **Continue** button.

e) In **LAN IP Address** entry, enter the public IP address of ELAN3-ALARM device and click **Continue** button.

f) By default, upon the successfully established connection, the system will prompt for an installer code.

g) By entering a valid installer code, the system grants access to full configuration remotely.

h) **Remote Configuration Management** window displays all performed configuration actions and connectivity information.



REMOTE CONNECTION

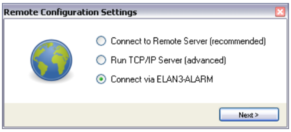
Server Type: Not Running

Device Status: --

Device Type: --

Firmware Version: --

Current State: --

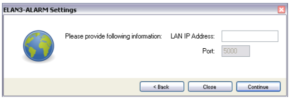


Remote Configuration Settings

○ Connect to Remote Server (recommended)

○ Run TCP/IP Server (advanced)

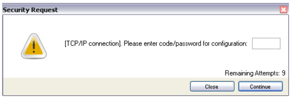
● Connect via ELAN3-ALARM



ELAN3-ALARM Settings

Please provide following information: LAN IP Address:

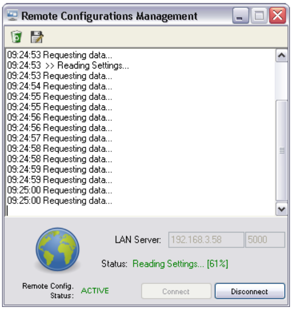
Port: 5000



Security Request

[TCP/IP connection]. Please enter code/password for configuration:

Remaining Attempts: 9



Remote Configurations Management

```
09:24:53 Requesting data...
09:24:53 >> Reading Settings...
09:24:53 Requesting data...
09:24:54 Requesting data...
09:24:55 Requesting data...
09:24:55 Requesting data...
09:24:56 Requesting data...
09:24:56 Requesting data...
09:24:57 Requesting data...
09:24:58 Requesting data...
09:24:58 Requesting data...
09:24:59 Requesting data...
09:24:59 Requesting data...
09:25:00 Requesting data...
09:25:00 Requesting data...
```

LAN Server: 192.168.3.58 5000

Status: Reading Settings... [61%]

Remote Config. Status: ACTIVE

5.4.3. Ending the Configuration Process

GPRS

ELAN3 ALARM

After the system configuration is complete, use one of the following methods to end the configuration process:

- Click **Disconnect** or **Stop** button and close *ELDES Configuration Tool* software;
- The session will automatically expire in 20 minutes. Before the last 5 minutes, the software will offer the user to extend the session for another 20 minutes.
- Alternatively, the connection with the server can be terminated at any time by sending an SMS text message.

Shut down the Connection with the Server

SMS text message content:
ssss_ENDCONFIG
Value: *ssss* – 4-digit SMS password.
Example: *1111_ENDCONFIG*

Once the session is expired or terminated, the system will reply with an SMS text message confirming the end of the session.

6. SMS PASSWORD AND INSTALLER CODE

For security reasons, the system uses the following type of password and code:

SMS password - 4-digit password used for system arming/disarming and configuration by SMS text messages. By default, SMS password is 0000, which MUST be changed!. SMS password is authorized to carry out the following:

- Access system configuration by SMS text messages.
- Arm/disarm partition.
- Activate/deactivate service mode.
- Set system date and time.
- Add/remove user phone numbers.
- Set SMS password.
- Turn ON/OFF PGM outputs.
- Restart system remotely.

Installer code – 4-digit password used for system configuration by EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software. By default, installer code is 1470, which is highly recommended to change. Installer code is authorized to carry out the following:

- Access system configuration by keypad and *ELDES Configuration Tool* software.
- Set installer code.
- Set master code.
- Activate/deactivate service mode.
- Set system date and time.
- Add/remove user phone numbers.
- Set SMS password.
- Turn ON/OFF PGM outputs.
- Restore system configuration to default.
- Clear tamper fault (if enabled).

Set SMS password

SMS

SMS text message content:
wwww_PSW_ssss
Value: *wwww* – 4-digit existing SMS password; *ssss* – 4-digit new SMS password; range – [0001... 9999].
Example: *0000_PSW_1111*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → SMS PASSWORD → OK → ssss → OK
Value: *iiii* **–** 4-digit installer code; *ssss* – 4-digit new SMS password; range – [0001... 9999].

EKB3/ EKB3W

Enter parameter 14 & new SMS password:
14 ssss #
Value: *ssss* – 4-digit new SMS password; range – [0001... 9999].
Example: *141111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set installer code

EKB2

Menu path:
OK → 1470 → OK → PRIMARY SETTINGS → OK → INSTALLER CODE → OK → iiii → OK
Value: *iii* – 4-digit new installer code; range – [0000... 9999].

EKB3/ EKB3W

Enter parameter 16 & new installer code:
16 iiii #
Value: *iii* – 4-digit new installer code; range – [0000... 9999].
Example: *162538#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

EN50131-1 **GRADE 3**

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All codes and passwords must consist of 6 digits.
- The system must prompt for master (see **10. MASTER AND USER CODES**) and installer (see **6. SMS PASSWORD AND INSTALLER CODE**) codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool software*.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **36. EN 50131-1 GRADE 3.**

7. SYSTEM LANGUAGE

The system comes equipped with a single language for communication with the user by SMS text messages and EKB2 keypad menu display. The system language depends on ESIM364 firmware, which is based on the user's location.

List of currently available system languages (firmwares):

- Czech
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hungarian
- Italian
- Latvian
- Lithuanian
- Polish
- Portuguese
- Romanian
- Russian
- Slovak
- Spanish

NOTE: To obtain a firmware that features a different SMS and EKB2 menu language, please contact your local dealer.

8. USER PHONE NUMBERS

The system supports up to 10 user phone numbers identified as User 1 through 10. When the phone number is set, the user will be able to arm/disarm the system by SMS text messages and free of charge phone calls (see **12.1. Free of Charge Phone Call** and **12.2. SMS Text Message**) as well as to configure the system by SMS text messages. User phone numbers are also used to receive alarm phone calls via GSM connection and SMS text messages from the system (see **17. ALARM INDICATIONS AND NOTIFICATIONS**).

By default, the system ignores any incoming calls and SMS text messages from a non-preset phone number as well as it rejects the SMS text messages containing wrong SMS password even from a preset user phone number (see **8.2. System Control from any Phone Number**).

To set User 1 phone number is mandatory, while the other 9 are optional. The supported phone number formats are the following:

- **International (with plus)** – The phone numbers must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for UK: +4417091111111. This format can be used when setting up the phone number by SMS text message and *ELDES Configuration Tool* software.
- **International (with 00)** – The phone numbers must be entered starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for UK: 004417091111111. This format can be used when setting up the phone number by SMS text message, EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software.
- **Local –** The phone numbers must be entered starting with an area code in the following format: [area code][local number], example for UK:017091111111. This format can be used when setting up the phone number by SMS text message, EKB2/ EKB3/EKB3W keypad and *ELDES Configuration Tool* software.

Add user phone number

SMS

SMS text message content:
ssss_NRup:ttteeellnnuumm
Value: *ssss* – 4-digit SMS password; *up* – user phone number slot, range – [1... 10]; *ttteeellnnuumm* – up to 15 digits user phone number.
Example: *1111_NR1:+4417091111111*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → GSM USER 1... 10 → OK → PHONE NUMBER → OK → ttteeellnnuumm → OK
Value: *iiii* – 4-digit installer code; *ttteeellnnuumm* – up to 15 digits user phone number.

EKB3/ EKB3W

Enter parameter 17, user phone number slot & phone number:
17 up ttteeellnnuumm #
Value: *up* – user phone number slot, range – [01... 10]; *ttteeellnnuumm* – up to 15 digits user phone number.
Example: *1701004417091111111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View user phone number

SMS

SMS text message content:
ssss_HELPNR
Value: *ssss* – 4-digit SMS password.
Example: *1111_HELPNR*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → GSM USER 1... 10 → OK → PHONE NUMBER
Value: *iiii* – 4-digit installer code;

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete user phone number

SMS

SMS text message content:
ssss_NRup:DEL
Value: *ssss* – 4-digit SMS password; *up* – user phone number slot, range – [2... 10].
Example: *1111_NR2:DEL*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → GSM USER 2... 10 → OK → PHONE NUMBER → OK → OK
Value: *iiii* – 4-digit installer code;

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: NEVER add a phone number of the device's SIM card as a user phone number!

ATTENTION: Once User 1 phone number is set, it will be restricted to modify it only.

NOTE: Multiple user phone numbers can be set by a single SMS text message, **Example:** *1111_NR1:+4417091111111_NR2:+4417091111112_NR6:017091111113_NR10:+4417091111114*

NOTE: Multiple user phone numbers can be deleted by a single SMS text message, **Example:** *1111_NR2:DEL_NR3:DEL_NR6:DEL_NR9:DEL_NR:10:DEL*

8.1. User Phone Number Names

When the system is armed or disarmed by free of charge phone call or SMS text message, the system sends a confirmation by SMS text message to user phone number that the system arming/disarming was initiated from. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the user phone number.

Manage user phone number name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

8.2. System Control from any Phone Number

By default, the system ignores any incoming calls and SMS text messages from a non-preset phone number as well as it rejects the SMS text messages containing wrong SMS password even from a preset user phone number. To allow/disallow system arming/disarming by phone call and SMS text messages that contain a valid SMS password from any phone number, please refer to the following configuration methods.

Enable system control from any phone number

SMS

SMS text message content:
ssss_STR:ON
Value: *ssss* – 4-digit SMS password.
Example: *1111_STR:ON*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CTRL FROM ANY NUM → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code;

EKB3/ EKB3W

Enter parameter 12 & parameter status value:
121#
Example: *121#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable system control from any phone number

SMS

SMS text message content:
ssss_STR:OFF
Value: *ssss* – 4-digit SMS password.
Example: *1111_STR:OFF*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CTRL FROM ANY NUM → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code;

EKB3/ EKB3W

Enter parameter 12 & parameter status value:
12 0 #
Example: *120#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

9. DATE AND TIME

The system comes equipped with internal real-time clock (RTC) that keeps track of the current date and time. Once the system is up and running, the user must set the correct date and time, otherwise the system will not operate properly. By default, after shutting down and starting up the system, the date and time must be set again.

Set date and time

SMS

SMS text message content:
ssss_yyyy.mt.dd_hr:mn
Value: *ssss* – 4-digit SMS password; *yyyy* – year; *mt* – month, range – [01... 12]; *dd* – day, range – [01... 31]; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59].
Example: *1111_2014.03.16_14:33*

EKB2

Menu path:
a) OK → uumm → OK → DATE/TIME SETTINGS → OK → yyyy-mt-dd hr:mn → OK
b) OK → iiii → OK → PRIMARY SETTINGS → OK → DATE/TIME SETTINGS → OK → yyyy-mt-dd hr:mn → OK
Value: *uumm* – 4-digit user/master code; *yyyy* – year; *mt* – month, range – [01... 12]; *dd* – day, range – [01... 31]; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59]; *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 66, date & time:
66 yyyy mt dd hr mn#
Value: *yyyy* – year; *mt* – month, range – [01... 12]; *dd* – day, range – [01... 31]; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59].
Example: *66201405291235#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: When the system is connected to the monitoring station via GPRS network connection (see **30. MONITORING STATION**) and/or when Smart Security feature is in use (see **37. SMART SECURITY**), the date and time will be automatically synchronized with the monitoring station or Smart Security server upon the system startup.

9.1. Automatic Date and Time Synchronization

This feature enables the system to set the date and time automatically without the user being involved in this process. The system supports the following methods of automatic date and time synchronization that are used automatically on system start-up and periodically (by default – every 30 days):

- **Via GSM network** – Once enabled, the system automatically sends a date/time request to the GSM operator. This method is the most accurate synchronization method. Some GSM operators might not support it.
- **By SMS text message** – Once enabled, the system automatically sends the SMS text message to its own phone number and retrieves the date and time from the SMS text message reply, as the included date and time is set by the SMSC (SMS center). This method is not as accurate as the synchronization via GSM network, but always effective.

By default, synchronization via GSM network is disabled. To enable/disable automatic date and time synchronization via GSM network, please refer to the following configuration methods.

Enable/disable synchronization via GSM network

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, synchronization by SMS text message is disabled. To enable/disable automatic date and time synchronization by SMS text message, please enter/remove device phone number using one of the following configuration methods.

Enter/remove device phone number for synchronization by SMS text message

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

10. MASTER AND USER CODES

ATTENTION: User/master code management must be carried out using master code and without Configuration mode being activated by the EKB3/EKB3W keypad.

NOTE for EKB3/EKB3W: User/master code management must be carried out using master code and without Configuration mode being activated by the EKB3/EKB3W keypad.

NOTE for EKB3/EKB3W: Master code management cat be carried out using an existing master code and without Configuration mode being activated or by activating Configuration mode using the installer code.

The system supports up to 30 numeric codes, identified as Master code and User code 1 through 29, allowing to carry out system arming/disarming as well as minor system configuration and control by the keypad.

Master code is authorized to carry out the following:

- Arm/disarm partition.
- Bypass violated zones.
- View violated zones and tampers.
- View system faults.
- Set system date and time.
- View temperature sensor information.
- View event log,
- View and clear alarm log,
- Set/delete user codes.
- Assign user code as Duress code.
- Assign user code as SGS code.

User code is authorized to carry out the following:

- Arm/disarm partition.
- Bypass violated zones.
- View violated zones and tampers.
- View system faults.
- Set system date and time.
- View temperature sensor information.
- View and clear alarm log.

By default, only Master code is preset as 1111 and assigned to Partition 1, 2, 3 and 4. For more details regarding User/Master code partition, please refer to **23.4. User/Master Code Partition.**

Set master code

EKB2

Menu path:
a) OK → vvvv → OK → CODES → OK → MASTER CODE → OK → → CODE → OK → mmmm → OK
b) OK → iiii → OK → PRIMARY SETTINGS → OK → MASTER CODE → mmmm → OK
Value: *vvvv* – 4-digit existing master code, range – [0000… 9999]; *iiii* – 4-digit installer code; *mmmm* – 4-digit new master code, range – [0000… 9999].

EKB3/EKB3W

a) Press [CODE], [0], enter existing master code & new master code:
[CODE] [0] vvvv 01 mmmm #
Value: *vvvv* - 4-digit existing master code; *mmmm* - 4-digit new master code; range - [0000… 9999].
Example: CODE01111012222#

b) Enter parameter 63, existing master code & new master code:
63 vvvv mmmm #
Value: *vvvv* – 4-digit existing master code; *mmmm* – 4-digit new master code, range – [0000… 9999].
Example: 6311112222#

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set user code

EKB2

Menu path:
User code 2... 16: OK → mmmm → OK → CODES → OK → USER CODE (2-16) → OK → USER CODE 2... 16 → OK → CODE → OK → uuuu → OK
User code 17... 30: OK → mmmm → OK → CODES → OK → USER CODE (17-30) → OK → USER CODE 17... 30 → OK → CODE → OK → uuuu → OK
Value: *mmmm* – 4-digit master code; *uuuu* – 4-digit user code, range – [0000... 9999].

EKB3/ EKB3W

Press [CODE], [0], enter master code, user code slot & user code:
[CODE] [0] mmmm us uuuuu #
Value: *mmmm* - 4-digit master code; *us* - user code slot, range - [02... 30]; *uuuu* - 4-digit user code, range - [0000... 9999].
Example: *CODE01111092556#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete user code

EKB2

Menu path:
OK → mmmm → OK → CODES → OK → REMOVE CODE → OK → uuuu → OK
Value: *mmmm* – 4-digit master code; *uuuu* – 4-digit user code.

EKB3/ EKB3W

Press [CODE], [0], enter master code & user code slot:
[CODE] [0] mmmm us #
Value: *mmmm* - 4-digit master code; *us* - user code slot, range - [02... 30].
Example: *CODE0111109#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The system does not allow to set a duplicate code.

Master code or one of the user codes ranging from User code 2 through 9 can be set as SGS (Security Guard Service) code, which is used for system arming/disarming by a security service employee. When used, the SGS code will be identified by a unique Contact ID code in the monitoring station.

Set SGS code

EKB2

Menu path:
Master code: OK → mmmm → OK → CODES → OK → SGS CODE → OK → N/A | MASTER CODE → OK
User code: OK → mmmm → OK → CODES → OK → SGS CODE → OK → N/A | USER CODE 2...10 → OK
Value: *mmmm* – 4-digit master code; *N/A* – SGS code not in use.

EKB3/ EKB3W

Press [CODE], [4], user code slot & enter master code:
Master code: [CODE] [4] 01 mmmm #
User code: [CODE] [4] us mmmm #
Value: *us* - user code slot, range - [02... 30]; *mmmm* - 4-digit master code.
Example: *CODE4041111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The Duress code is used when system disarming is demanded by force. When used, the system will disarm as well as it will silently transmit an alert to the monitoring station. Only Master code one of the user codes ranging from User code 2 through 9 can be set as Duress code.

Set Duress code

EKB2

Menu path:
Master code: OK → mmmm → OK → CODES → OK → DURESS CODE → OK → N/A |MASTER CODE → OK
User code: OK → mmmm → OK → CODES → OK → DURESS CODE → OK → N/A | USER CODE 2... 10 → OK
Value: *mmmm* – 4-digit master code; *N/A* – Duress code not in use.

EKB3/ EKB3W

Press [CODE], [3], 01/user code slot & enter master code:
Master code: [CODE] [3] 01 mmmm #
User code: [CODE] [3] us mmmm #
Value: *us* - user code slot, range - [02... 30]; *mmmm* - 4-digit master code.
Example: *CODE3081111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

EN50131-1 **GRADE 3**

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All codes and passwords must consist of 6 digits.
- The system must prompt for master (see **10. MASTER AND USER CODES**) and installer (see **6. SMS PASSWORD AND INSTALLER CODE**) codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool software*.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **36. EN 50131-1 GRADE 3.**

10.1. Master and User Code Names

When the system is armed or disarmed by entering a master or user code using a keypad, the system sends a confirmation by SMS text message to user phone number, sharing the same partition (-s) as the keypad and user/master code. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the user/master code.

Manage user/master code name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

11. iBUTTON KEYS

An iButton key is a unique 64-bit ID code containing chip enclosed in a stainless steel tab usually implemented in a small plastic holder. ESIM364 system supports up to 16 iButton keys each holding a unique identity code (ID), which is used for system arming and disarming.

11.1. Adding and Removing iButton Keys

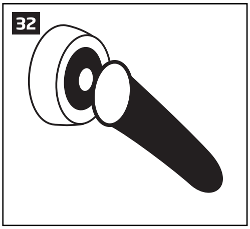
To add an iButton key to the system, do the following:

a) Disarm the system in all partitions (see **12. ARMING AND DISARMING**).

b) Enable Allow Adding New iButton Keys mode.

c) T ouch the key to the iButton key reader when the system is disarmed (see Fig. No. 32).

32



d) The successfully added iButton key will be indicated by short beeps emitted by the system's buzzer.

e) Add as many iButton keys as necessary – touch one key after another to the reader – until the number of 16 keys is reached.

NOTE: iButton Key 1 can be added without Allow Adding New iButton Keys mode being enabled.

Enable Allow Adding New iButton Keys mode

SMS	**SMS text message content:** ssss_IBPROG:ON **Value:** *ssss* – 4-digit SMS password. **Example:** *1111_IBPROG:ON*
EKB2	**Menu path:** OK → iiii → OK → IBUTTON KEYS → OK → NEW IBUTTON → OK → ENABLE → OK **Value:** *iiii* - 4-digit installer code.
EKB3/ EKB3W	**Enter parameter 18 & parameter status value:** 18 0 # **Example:** *180#*
Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

When adding of iButton keys is complete, please disable Allow Adding New iButton Keys mode.

Disable Allow Adding New iButton Keys mode

SMS

SMS text message content:
ssss_IBPROG:OFF
Value: *ssss* – 4-digit SMS password.
Example: *1111_IBPROG:ON*

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → NEW IBUTTON → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 18 & parameter status value:
181 #
Example: *181#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To view the ID of the added iButton keys, please refer to the following configuration methods.

View iButton key ID

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → IBUTTON → OK → IBUTTON 1...16 → OK → ID
Value: *iiii* - 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If the iButton key is lost or stolen, due to security reasons it is highly recommended to remove it from the system.

Remove individual iButton key from the system

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → IBUTTON → OK → IBUTTON 1...16 → OK → REMOVE → OK
Value: *iiii* - 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Remove all iButton keys from the system

SMS

SMS text message content:
ssss_RESETIB
Value: *ssss* – 4-digit SMS password.
Example: *1111_RESETIB*

11.2. iButton Key Names

When the system is armed or disarmed by iButton key, the system sends a confirmation by SMS text message to preset user phone number, sharing the same partition (-s) as the key. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the iButton key.

Manage iButton key name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

12. ARMING AND DISARMING

The system features the following methods to carry out arming and disarming process:

- Free of charge phone call.
- SMS text message.
- EKB2/EKB3/EKB3W keypad and user/master code.
- iButton key.
- EWK1/EWK2 wireless keyfob.
- Arm-Disarm by Zone.
- EGR100 middle-ware.

The system arms/disarms the partitions that the preset user phone number, EKB2/EKB3/EKB3W keypad and user/master code, iButton key, EWK1/EWK2 wireless keyfob or zone, set up for Arm-Disarm by Zone method, are assigned to. For example, if User 1 phone number is assigned to Partition 1, 2 and 4, the user will be able to arm/disarm Partition 1, 2 and 4 by a single phone call to the system (see **23. PARTITIONS**).

By default, when the system is successfully armed or disarmed, it replies with confirmation by SMS text message. For more details on SMS text message regarding system arming/disarming and how to manage it, please refer to **12.9. Disabling and Enabling Arm/Disarm Notifications**.

The system will allow to arm the system if the following system faults are present (see **29. INDICATION OF SYSTEM FAULTS**):

- Main power supply is lost.
- Low battery.
- Battery dead or missing.
- Battery failed.
- Siren failed.
- Date/time not set.
- GSM connection failed.
- GSM/GPRS antenna failed.
- Wireless antenna failed.
- Keypad lost.

When attempting to arm the system (by any method, except EKB2/EKB3/EKB3W keypad and user/master code, EGR100 middle-ware) in case of violated zone/tamper presence, the system will reply with SMS text message containing violated zone/tamper number. Due to security reasons it is highly recommended to restore the violated zone/tamper before arming the system. For more details on how to arm the system despite the violated zone presence, please refer to **14.6. Zone Attributes** and **14.7. Bypassing and Activating Zones.**

The system ignores any incoming calls and SMS text messages from a non-preset phone number as well as it rejects the SMS text messages containing wrong SMS password even from a preset user phone number. For more details regarding arming/disarming the system from a non-preset phone number, please refer to **8.2. System Control from any Phone Number**.

NOTE: The system remembers the last status (armed/disarmed) of all partitions even after complete shut down.

EN50131-1 **GRADE 3**

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following feature:

- System arming is blocked if any system fault exists. The user will not be able to arm the system until all existing system faults are solved.
- System arming is blocked until tamper fault is cleared by the installer.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **36. EN 50131-1 GRADE 3.**

12.1. Free of Charge Phone Call

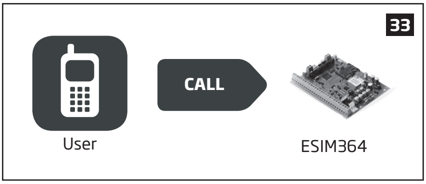
To arm and disarm the system, dial the system's phone number from any of 10 available user phone numbers (see **8. USER PHONE NUMBERS** for user phone number management). The phone call is free charge as the system rejects it and carries out arming/disarming procedure afterwards. When arming – the system rejects the phone call after 2 rings, when disarming – the system rejects the phone call immediately. If there is more than one preset user dialing to the system at the same time, the system will accept the incoming call from the user who was the first to dial while other user (-s) will be ignored.

When system's phone number is dialed for arming, the system will proceed as follows:

- Non-partitioned system:
  - If ready (no violated zone/tamper), the system will arm.
  - If unready (violated zone/tamper is present), the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number.

- Partitioned system:
  - If all partitions are disarmed ready, the system will arm them.
  - If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). The system will then send an SMS text message, containing a list of violated zones/tampers, to user phone number that the system arming was initiated from.
  - If a combination of armed and disarmed ready partitions is present, the system will arm the disarmed ready partitions and skip the armed ones.

When a user phone number is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by dialing the system's phone number. For example, if User 1 is assigned to Partition 1, 2 and 3, the user will be able to arm/disarm Partition 1, 2 and 3 by a single phone call to the system from User 1 phone number. For more details on how to set user phone number partition, please refer to **23.2. User Phone Number Partition**.


33

12.2. SMS Text Message

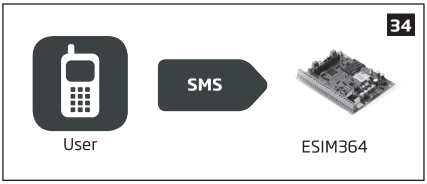
SMS

To arm the system by SMS text message, send the following text to the system's phone number from any of 10 available user phone numbers (see **8. USER PHONE NUMBERS** for user phone number management). When the SMS text message for arming is sent to the system's phone number, the system will proceed as follows:

- Non-partitioned system:
  - If ready (no violated zone/tamper), the system will arm.
  - If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number.
- Partitioned system:
  - If all partitions are disarmed ready (no violated zone/tamper), the system will arm them.
  - If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). The system will then send an SMS text message, containing a list of violated zones/tampers, to user phone number that the system arming was initiated from.
  - If a combination of armed and disarmed ready partitions is present, the system will arm the disarmed ready partitions and skip the armed ones.

Arm the system

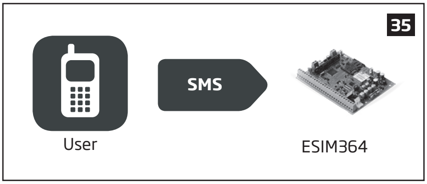
SMS text message content:
ssss_ARMp or ssss_ARMp,p,p,p
Value: *ssss* – 4-digit SMS password; *p* – partition number, range – [1... 4].
Example: *1111_ARM1*


34

To disarm the system by SMS text message, send the following text to the system's phone number from any of 10 available user phone numbers:

Disarm the system

SMS text message content:
ssss_DISARMp or ssss_DISARMp,p,p,p
Value: *ssss* – 4-digit SMS password; *p* – partition number, range – [1... 4].
Example: *1111_DISARM1,2,4*



When a user phone number is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by sending the SMS text message to the system's phone number. For example, if User 3 is assigned to Partition 2 and 3, the user will be able to arm/disarm Partition 2 and/or 3 by sending an SMS text message from User 3 phone number. For more details on how to set user phone number partition, please refer to **23.2. User Phone Number Partition**.

12.3. EKB2 Keypad and User/Master Code

✓ icon displayed next to the partition name in the home screen view of EKB2 keypad indicates that no violated zones and/or tampers are present, therefore the partition is ready for arming. If ✗ icon is displayed instead, the partition is unready for arming, therefore the user must restore all violated zones and/or tampers before arming the partition. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**). ⚠ icon appears in the home screen view if system fault (-s) exist (see **29. INDICATION OF SYSTEM FAULTS**).

To arm the system by EKB2 keypad, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad (see **10. MASTER AND USER CODES** for user/master code management). By default, the arming process is as follows:

Non-partitioned system:

a) When a valid user or master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps, the keypad will switch to home screen view and display the countdown timer.

b) When a valid user or master code is entered, the keypad will display the partition selection menu. Once the partition is selected, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow. If ⬅ key is touched twice during exit delay, the keypad will return to home screen view and display the countdown timer next to the partition name .

When successfully armed:

- by default, the countdown timer will disappear.
- in addition, if enabled, the keypad will display 🔒 icon next to the partition name that has been armed.

Partitioned system; arming a single partition as the keypad is assigned to – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow. If ⬅ key is touched twice during exit delay, the keypad will return to home screen view and display the countdown timer next to the partition name that is being armed. When successfully armed:

- by default, the countdown timer will disappear.
- in addition, if enabled, the keypad will display 🔒 icon next to the partition name that has been armed.

Partitioned system; arming a different single partition than the keypad is assigned to – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the system will initiate exit delay, but will not indicate it on EKB2 keypad due to the difference between keypad partition and the one being armed. Then the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow. Alternatively, the ⬅ key may be touched in order to instantly return to home screen view.
Partitioned system; arming multiple partitions simultaneously – When a valid user or master code is entered, the keypad will display the partition selection menu. Once **ARM ALL** menu item is selected the system will proceed as follows:

- if all partitions are disarmed-ready (no violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display multiple **ARMING part-name** messages for 3 seconds reflecting each partition the user/master code is assigned to, followed by partition selection menu.
- if one or more partitions are disarmed-unready (contains violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message (-s) reflecting ready partition (-s), while the unready partition (-s) will be skipped indicated by **part-name NOT READY** message (-s) followed by partition selection menu. Each message will be displayed for 2 seconds and corresponds to the partition (-s) the user/master code is assigned to.
- if a combination of armed and disarmed-ready partitions exist, the system will initiate exit delay. During the exit delay, the keypad's

buzzer will emit short beeps and the keypad will display **ARMING part-name** message (-s) seconds reflecting ready partition (-s), while the pre-armed partition (-s) will be skipped. Each message will be displayed for 2 seconds and corresponds to the partition (-s) the user/master code is assigned to.

When the keypad back-light timeout expires, the home screen view will follow. If key ⬅ is touched twice during exit delay, the keypad will return to home screen view and display the countdown timers next to the partition names the keypad is assigned to. When successfully armed:

- by default, the countdown timers will disappear.
- in addition, if enabled, the keypad will display 🔒 icon next to the partition name that has been armed.

Arm the system

Enter user/master code (and select partition):
Non-partitioned system:
a) uumm → OK
b) OK → uumm → OK → ARM/DIS PARTITION → OK → [p] part-name → OK
Partitioned system – arming a single partition: uumm → OK → [p] part-name → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → [p] part-name → OK
Partitioned system – arming multiple partitions: uumm → OK → ARM ALL → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → ARM ALL → OK
Value: *uumm* – 4-digit user/master code; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name.

To cancel the arming process:

- Non-partitioned system – Enter the user/master code again during exit delay countdown.
- Partitioned system – Select the partition again, that is currently being armed, from the partition selection menu during exit delay countdown. The keypad will display part-name ARMING TERMINATED message for 2 seconds followed by partiton selection menu.

To disarm or turn OFF the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad. By default, the system disarming process is as follows:

Non-partitioned system:

a) When a valid user or master code is entered, the keypad will switch to home screen view.

b) When a valid user or master code is entered, the keypad will display the partition selection menu. Once the partition is selected, the keypad will display **part-name DISARMED** message for 3 seconds and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the ⬅ ikonas key may be touched in order to instantly return to home screen view.

Partitioned system; disarming a single partition – When a valid user or master code is entered, the keypad will display the partition selection menu. Once a partition that is to be disarmed is selected, the keypad will display **part-name DISARMED** message for 2 seconds and return to partition selection menu followed by home screen view after the keypad back-light timeout expires.

Partitioned system; disarming multiple partitions simultaneously – When a valid user or master code is entered, the keypad will display the partition selection menu. Once **DISARM ALL** menu item is selected, the keypad will display multiple **part-name DISARMED** messages for 2 seconds reflecting each partition the user/master code is assigned to and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the ⬅ ikonas key may be touched in order to instantly return to home screen view.

Disarm the system

Enter user/master code (and select partition):
Non-partitioned system:
a) uumm → OK
b) OK → uumm → OK → ARM/DIS PARTITION → OK → [p] part-name → OK
Partitioned system – disarming a single partition: uumm → OK → [p] part-name → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → [p] part-name → OK
Partitioned system – disarming multiple partitions: uumm → OK → ARM ALL → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → ARM ALL → OK
Value: *uumm* – 4-digit user/master code; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name.

When a user/master code is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by EKB2 keypad using partition selection menu. However, if a user/master code is assigned to Partition 1, 2 and 4, while EKB2 keypad is assigned to Partition 2, the user will be able to arm/disarm Partition 1, 2 and 4, but the keypad will only display Partition 2 name and the related information in home scren view. For more details on how to set keypad partition and user/master code partition, please refer to **23.4. User/Master Code Partition.**

Enable/disable Show ARMED status in keypad

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: If the user fails to enter a correct user/master code 10 times in a row, the system will block the keypad for 2 minutes and the keypad will display **KEYPAD BLOCKED** message. While the keypad is blocked, the system prevents from entering any user/master code. The keypad will automatically unblock once the 2-minute time has expired and display **KEYPAD UNBLOCKED** message.

NOTE: The keypad will display 🔒 icon and 🔓 icon next to the armed and disarmed partition name in home screen view respectively only if **Show ARMED status in keypad** parameter is enabled and the keypad is assigned to the same partition (-s) as the armed/disarmed one.

12.4. EKB3 Keypad and User/Master Code

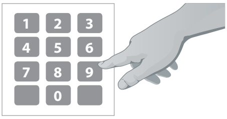
ATTENTION: EKB3 keypad can operate either in 2-partition or in 4-partition mode. The description of the following procedure is based on 4-partition mode operation on EKB3 keypad. The arming/disarming procedure in 2-partition mode using EKB3 keypad would be carried out identically to EKB3W wireless keypad. For more details on 2-partition mode, please refer to **12.5. EKB3W Keypad and User/Master Code**

Illuminated indicator READY on EKB3 keypad indicates that no violated zones and/or tampers are present, therefore the partition is ready for arming. If the indicator READY is not illuminated, the partition is unready for arming, therefore the user must restore all violated zones and/or tampers before arming the partition. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**). Indicator SYSTEM will illuminate or flash if system fault (-s) exist (see **29. INDICATION OF SYSTEM FAULTS**).

To arm the system by EKB3 keypad, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad (see **10. MASTER AND USER CODES** for user/master code management). By default, the arming process is as follows:

Non-partitioned system/Partitioned system; arming a single partition as the keypad is assigned to – When a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system



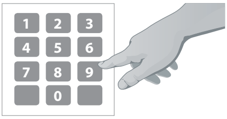
Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code
Example: *2222*

Partitioned system; arming a different single partition than the keypad is assigned to – To arm a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled; see **23.3. Keypad Partition and Keypad Partition Switch**) before arming process. Once the partition is swiched and a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Use keypad partition switch

Hold the [1]... [4] key and release it after 3 short beeps:
Value: [1]... [4] key – parition number 1... 4

Arm the system

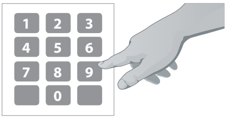


Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code
Example: *2222*

Partitioned system; arming multiple partitions simultaneously – If a user/master code assigned to all 4 partitions exist, user can arm all partitions simultaneously. When this feature is used, the system will proceed as follows:

- if all partitions are disarmed-ready (no violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and indicator ARMED along with number [1], [2], [3] and [4] keys will light ON. When the system is successfully armed, the keypad's buzzer will silent down.
- if one or more partitions are disarmed-unready (keypad number [1]... [4] key flashing, indicating the partition that contains violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and keypad indicator ARMED (if the keypad is switched to a non-violated partition) along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. The ready partition (-s) will be armed and the unready one (-s) will be skipped.
- if a combination of armed and disarmed ready partitions is present, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and keypad indicator ARMED (if the keypad is switched to a disarmed partition) along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. The disarmed-ready partitions will be armed and the pre-armed ones will be skipped.

Arm all 4 partitions simultaneously



Hold the [0] key, release it after 3 short beeps and enter user/master code:
0 uumm
Value: *uumm* – 4-digit user/master code.
Example: *0 2222*

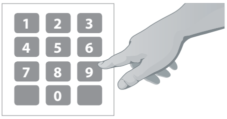
The system will arm/disarm the partition corresponding to the one that user/master code (see **23.4. User/Master Code Partition**) and the keypad (see **23.3. Keypad Partition and Keypad Partition Switch**) are assigned to. For example, if User code 4 is assigned to Partition 2, 3 and 4, while EKB3 keypad is assigned to Partition 2, the user will be able to arm/disarm only Partition 2 by entering User code 4.

To cancel the arming process, enter the user/master code again during exit delay countdown.

To disarm or turn OFF the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad. By default, the system disarming process is as follows:

Non-partitioned system/Partitioned system; disarming a single partition as the keypad is assigned to – When a valid user/master code is entered, indicator ARMED and the number [1]... [4] key, indicating the partition that has been disarmed, will light OFF.

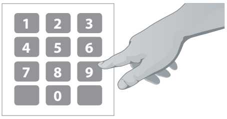
Disarm the system



Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code
Example: *222*

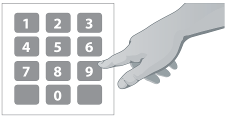
Partitioned system; disarming a different single partition than the keypad is assigned – To disarm a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled; see **23.3. Keypad Partition and Keypad Partition Switch**) before disarming process. Once the partition is swiched and a valid user/master code is entered, indicator ARMED and the number [1]... [4] key, indicating the partition that has been disarmed, will light OFF.

Use keypad partition switch



Hold the [1]... [4] key and release it after 3 short beeps:
Value: [1]... [4] key – parition number 1... 4

Disarm the system

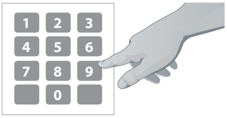


Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code
Example: *2222*

Partitioned system; disarming multiple partitions simultaneously – If a user/master code assigned to all 4 partitions exist, user can disarm all partitions simultaneously. When this feature is used, the system will proceed as follows:

- if all partitions are armed and a valid user/master code is entered, indicator ARMED along with the number [1], [2], [3] and [4] keys will light OFF.
- if a combination of armed and disarmed ready partitions is present, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and keypad indicator ARMED (if the keypad is switched to a disarmed partition) along with the number [1]... [4] key, indicating the partition that is to be armed, will light ON. The disarmed-ready partitions will be armed and the pre-armed ones will be skipped.
- if one or more partitions are disarmed-unready (keypad number [1]... [4] key flashing, indicating the partition that contains violated zone/tamper), the system will deny simultaneous partition disarming until the partition's zone/tamper violation is removed. Alternatively, the user can disarm the partitions one by one (see P**artitioned system; arming a different single partition than the keypad is assigned to above**).

Disarm all 4 partitions simultaneously



Hold the [0] key, release it after 3 short beeps and enter user/master code:
0 uumm
Value: *uumm* – 4-digit user/master code.
Example: *0 2222*

NOTE: To arm/disarm all partitions simultaneously, the user/master code must be assigned to all 4 partitions and the keypad partition switch feature enabled (see **23.3. Keypad Partition and Keypad Partition Switch**)..

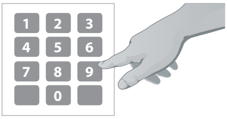
12.5. EKB3W Keypad and User/Master Code

Illuminated indicator READY on EKB3W keypad indicates that no violated zones and/or tampers are present, therefore the partition is ready for arming. If the indicator READY is not illuminated, the partition is unready for arming, therefore the user must restore all violated zones and/or tampers before arming the partition. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**). Indicator SYSTEM will illuminate or flash if system fault (-s) exist (see **29. INDICATION OF SYSTEM FAULTS**).

To arm the system by EKB3W keypad, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad (see **10. MASTER AND USER CODES** for user/master code management). By default, the arming process is as follows:

Non-partitioned system/Partitioned system; arming a single partition as the keypad is assigned to – When a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

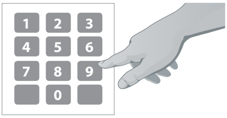
Arm the system



Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code
Example: 2222

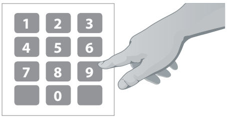
Partitioned system; arming a different single partition than the keypad is assigned to – To arm a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled; see **23.3. Keypad Partition and Keypad Partition Switch**) before arming process. Once the partition is swiched and a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Use keypad partition switch



Hold the [1]... [4] key and release it after 3 short beeps:
Value: [1]... [4] key – parition number 1... 4

Arm the system



Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code
Example: *2222*

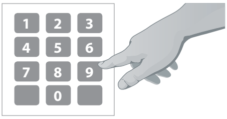
The system will arm/disarm the partition corresponding to the one that user/master code (see **23.4. User/Master Code Partition**) and the keypad (see **23.3. Keypad Partition and Keypad Partition Switch**) are assigned to. For example, if User code 4 is assigned to Partition 2, while EKB3W keypad is assigned to Partition 1, the user will be able to arm/disarm only Partition 2 by entering User code 4.

To cancel the arming process, enter the user/master code again during exit delay countdown.

To disarm or turn OFF the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad. By default, the system disarming process is as follows:

Non-partitioned system/Partitioned system; disarming a single partition as the keypad is assigned to – When a valid user/master code is entered, indicator ARMED will light OFF.

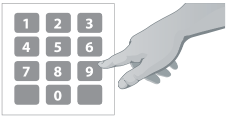
Disarm the system



Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

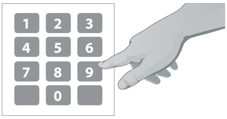
Partitioned system; disarming a different single partition than the keypad is assigned – To disarm a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled; see **23.3. Keypad Partition and Keypad Partition Switch**) before disarming process. Once the partition is swiched and a valid user/master code is entered, indicator ARMED will light OFF.

Use keypad partition switch



Hold the [1]... [2] key and release it after 3 short beeps:
Value: [1]... [2] key – parition number 1... 2

Disarm the system



Enter user/master code:
uumm
Value: *uumm* – 4-digit user/master code.
Example: *2222*

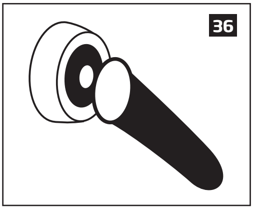
NOTE: The user can arm/disarm only the first two system partitions using EKB3W keypad.

12.6. iButton Key

To arm or disarm the system, touch the iButton key reader by any of 16 available iButton keys (see **11. iBUTTON KEYS** for iButton key management). When the iButton is touched to the iButton key reader for arming, the system will proceed as follows:

- **Non-partitioned system:**
  - If ready (no violated zone/tamper), the system will initiate exit delay and arm.
  - If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**).

- **Partitioned system:**
  - If all partitions are disarmed ready (no violated zone/tamper), the system will initiate exit delay and arm them.
  - If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). The system will then send an SMS text message, containing a list of violated zones/tampers, to user phone number, sharing the same partition (-s) as the iButton key. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**).
  - If a combination of armed and disarmed ready partitions is present, the system will initiate exit delay, arm the disarmed ready partitions and skip the armed ones.



36

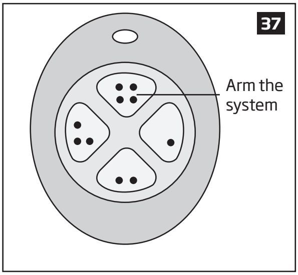
When an iButton key is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by touching the iButton key to the reader. For example, if iButton 5 is assigned to Partition 1 and 4, the user will be able to arm/disarm Partition 1 and 4 by touching iButton 5 to the reader. For more details on how to set iButton key partition, please refer to **23.5. iButton Key Partition**.

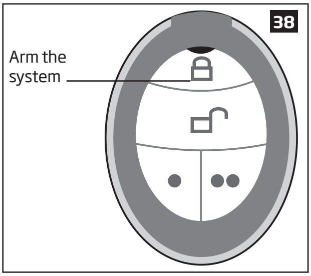
12.7. EWK1/EWK2 Wireless Keyfob

EWK1/ EWK2

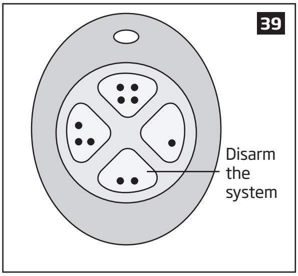
To arm the system, press 1 of 4 keyfob buttons set to arm the system (by default, EWK1 – ⁘ ;EWK 2 - 🔒). When EWK1/ EWK2 button is pressed for arming, the system will proceed as follows:

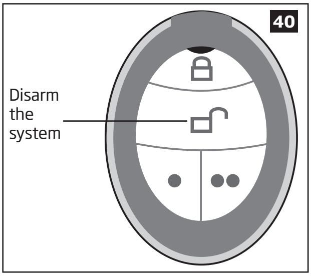
- **Non-partitioned/partitioned system:**
  - If all partitions are disarmed ready (no violated zone/tamper), the system will initiate exit delay and arm them.
  - If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zone**s), disabled (see **14.9. Disabling and Enabling Zone**s) or a Force attribute enabled (see **14.6. Zone Attributes**).


37


38

To disarm the system, press 1 of 4 keyfob buttons set to disarm the system (by default, EWK1 - •• ; EWK2 - 🔓).


39


40

To verify if the system has been successfully armed, do not release the *Arm the system* keyfob button and wait for the 3 short keyfob buzzer's beeps/indicator's flashes indicating the successfully carried out command. The long beep/flash indicates the unsuccessful command.

The system will arm/disarm the partition corresponding to the one that EWK1/EWK2 wireless keyfob is assigned to (see **23.6. EWK1/ EWK2 Wireless Keyfob Partition**). For example, if EWK1/EWK2 wireless keyfob is assigned to Partition 3, the user will be able to arm/ disarm only Partition 3. To arm a different partition than the EWK1/EWK2 wireless keyfob is assigned to, bind another EWK1/EWK2 keyfob to the system and assign it to a different partition.

For more details on how to manage EWK1/EWK2 keyfob buttons, please refer to *ELDES Configuration Tool* software's HELP section.

12.8. Arm-Disarm by Zone

ARM/ DISARM ZONE

The Arm-Disarm by Zone feature allows to use a zone for arming and disarming the alarm system when the zone is violated and restored. The process is performed by providing a low-level pulse for more than 3 seconds into the specified zone. It means that violating and restoring the zone leads to system arming and by repeating this action the system becomes disarmed. The system will arm/disarm the partition (-s) that the zone is assigned to. This method can be set up to 4 pn-board zones

Set zone for Arm-Disarm by Zone method

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ARM/DISARM BY ZONE → OK → ZONE 1... 4 → OK → nn
Value: *iiii* – 4-digit installer code; *nn* – on-board zone number, range – [01... 12].

EKB3/ EKB3W

Enter parameter 34, on-board zone slot & zone number:
34 z nn #
Value: *z* – on-board zone slot for Arm-Disarm by Zone method; range - [1... 4]; *nn* – on-board zone number, range – [01... 12].
Example: *34023#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Arm-Disarm by Zone method

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ARM/DISARM BY ZONE → OK → ZONE 1... 4 → OK → 0
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 34, on-board zone slot & parameter status value
Value: *z* – on-board zone slot for Arm-Disarm by Zone method; range - [1... 4].
Example: *34200#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

12.9. Disabling and Enabling Arm/Disarm Notifications

By default, when the system is successfully armed or disarmed, it replies with confirmation by SMS text message to:

- user phone number, sharing the same partition as EKB2/EKB3/EKB3W keypad and user/master code, iButton key, EWK1/EWK2 wireless keyfob or zone, set up for Arm/Disarm by Zone method.
- user phone number that the system arming/disarming by free of charge phone call was initiated from.
- user phone number that the system arming/disarming by SMS text message was initiated from.

The confirmation SMS text message is sent to the user phone number regarding each partition separately and contains system status and partition name as well as it may contain a user name assigned to user phone number, user/master code or iButton key. For more details on names, please refer to **8.1. User Phone Number Names, 10.1. User/Master Code Names** and **11.2. iButton Key Names.**

To disable/enable this notification for individual user phone number, please refer to the following configuration methods.

Disable arm/disarm notification

EKB2

Menu path:
System armed:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → SMS REPORT → OK → DISABLE → OK

System disarmed:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → SMS REPORT → OK → DISABLE→ OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
System armed event
User phone number: 25 01 up 0 #
SMS text message to all users simultaneously: 21 01 up 0 #
SMS delivery report: 55 01 up 0 #

System disarmed event
User phone number: 25 02 up 0 #
SMS text message to all users simultaneously: 21 02 up 0 #
SMS delivery report: 55 02 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2502040#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable arm/disarm notification

EKB2

Menu path:
System armed:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → SMS REPORT → OK → ENABLE → OK

System disarmed:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → SMS TO ALL → OK → ENBABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → SMS REPORT → OK → ENABLE → OK

Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
System armed event
User phone number 25 01 up 1 #

SMS text message to all users simultaneously: 21 01 up 1 #

SMS delivery report: 55 01 up1 #

System disarmed event
User phone number: 25 02 up 1 #

SMS text message to all users simultaneously: 21 02 up 1 #

SMS delivery report: 55 02 up 1 #

Value: *up* - user phone number slot, range - [01... 10].
Example: *2502061#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery* report parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

13. EXIT AND ENTRY DELAY

When arming, the system initiates the exit delay countdown (by default – 15 seconds) intended for the user to leave the secured area. The exit delay is indicated by short beeps emitted by EKB2/EKB3/EKB3W keypad buzzer and buzzer, connected to the alarm system. When arming:

- a non-partitioned system, a countdown timer will be displayed in the home screen view of EKB2 during exit delay.
- a partitioned system, EKB2 keypad will display **ARMING part-name** message on the screen for 2 seconds and switch to partition selection menu during exit delay.

Exit delay is provided when arming the system by the following methods:

- EKB2/EKB3/EKB3W keypad and user/master code.
- iButton key.
- EWK1/EWK2 wireless keyfob.
- Arm/Disarm by Zone.

To arm the system without exit delay, use one of the following system arming methods:

- Free of charge phone call.
- SMS text message.
- EGR100 middle-ware.

Set exit delay

SMS

SMS text message content:
ssss_EXITDELAY:p,ext or ssss_EXITDELAY:p,ext;p,ext;p,ext;p,ext
Value: *ssss* – 4-digit SMS password; *p* – partition number, range – [1... 4], *ext* – exit delay duration, range – [0... 600] seconds.
Example: *1111_EXITDELAY:1,20;3,43*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → EXIT DELAY → OK → PARTITION 1... 4 → OK → ext → OK
Value: *iiii* – 4-digit installer code;, *ext* – exit delay duration, range – [0... 600] seconds.

EKB3/ EKB3W

Enter parameter 72, partition number & exit delay duration:
72 pp ext #
Value: *pp* – partition number, range – [01... 04], *ext* – exit delay duration, range – [0... 600] seconds.
Example: *7203259#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Alternatively, you can set exit delay value to 0 in order to arm the system without exit delay by any available method.

NOTE: EKB3/EKB3W keypad buzzer will only beep if the keypad is operating in the partition where exit delay countdown is in progress.

Once the exit delay has expired, the system initiates the entry delay countdown (by default – 15 seconds) if a Delay type zone is violated. The countdown is indicated by short beeps emitted by keypad buzzer and by steady beep emitted by system's buzzer. The indication is intended to advise the user that the system should be disarmed. Once the user presses/touches any key on the keypad during this delay, the buzzer of the keypad will be silenced. If the system is disarmed before the entry delay expires, no alarm will be caused.

Set entry delay for Delay zone	**SMS**	**SMS text message content:** ssss_ENTRYDELAY:nn,eeeee or ssss_ENTRYDELAY:nn,eeeee;nn,eeeee;nn,eeeee;nn,eeeee **Value:** *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 76], *eeeee* – entry delay duration, range – [0... 65535] seconds. **Example:** *1111_ENTRYDELAY:1,25;54,14;12,20*
	EKB2	**Menu path:** On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → ENTRY DELAY → OK → eeeee → OK Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → ENTRY DELAY → OK → eeeee → OK Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → ENTRY DELAY → OK → eeeee → OK EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17... 32 → OK → EPGM1 ZONE 1... 32 → OK → ENTRY DELAY → OK → eeeee → OK **Value:** *iiii* – 4-digit installer code; *eeeee* – entry delay duration, range – [0... 65535] seconds.
	EKB3/ EKB3W	**Enter parameter 54, partition number and entry delay duration:** 54 nn eeeee # **Value:** *nn* – zone number, range – [01... 76], *eeeee* – entry delay duration, range – [0... 65535] seconds **Example:** *5403259#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Due to battery power saving reasons, EKB3W keypad buzzer will not sound during exit and entry delay if the violated Delay type zone is not of the associated EKB3W keypad.

For more details on zone types, please refer to **14.5. Zone Type Definitions**.

14. ZONES

Detection devices such as motion detectors and door contacts are connected to the alarm system's zone terminals. Once connected, the associated zone's parameters must be configured.

ESIM364 comes equipped with 6 on-board zones allowing to connect up to 6 detection devices. For more details regarding zone expansion, please refer to **14.2. Zone Expansion**.

ESIM364 zones are classified by 5 categories:

Zone category	Description	Max. number of zones per device	Max. number of zones in total
On-board zones	Built-in wired zones of ESIM364 alarm system.	6/12*	6/12*
Keypad zones	Hardwired zones of EKB2/EKB3 keypad.	1	4
EPGM1 zones	Zones of EPGM1 - hardwired zone & PGM output expansion module.	16	32
Wireless zones	Non-physical zones automatically created by connected wireless devices.	2**	64***
Virtual zones	Non-physical zones intended for Panic button feature (alarm activaton upon pressing the button) on EWK1/EWK2 wireless keyfob. Virtual zones can be manually created using *ELDES Configuration Tool* software.	64****	64****

* - 6-Zone mode is enabled by default. ATZ mode doubles the on-board zone number and increases it to 12 in total.
** - Depends on the connected wireless device.
*** - Available only if no zones, EPGM1 zones and virtual zones are present.
**** - Available only if no zones, EPGM1 zones and wireless zones are present.

14.1. Zone Numbering

The zone numbers ranging from Z1 through Z12 are permanently reserved for on-board zones even when ATZ mode is disabled. The Z13-Z76 zone numbers are automatically assigned in the chronological order to the created virtual zones and the devices connected to the system: keypads, wireless devices, EPGM1 modules.

14.2. Zone Expansion

For additional detection device connection, the number of zones can be expanded by:

- enabling the ATZ (Advanced Technology zone) mode (see **14.4. ATZ (Advanced Technology Zone) Mode**).
- connecting EPGM1 hardwired zone and PGM output expansion module (see **32.1.3. EPGM1 - Hardwired Zone & PGM Output Expansion Module**).
- connecting keypads (see **32.1.1. EKB2 - LCD Keypad**, **32.1.2. EKB3 - LED Keypad** and **33.1. EKB3W - Wireless LED Keypad**).
- binding wireless devices (see **19. WIRELESS DEVICES**).
- creating virtual zones (see *ELDES Configuration Tool* software's Help section).

The maximum supported number of zones is 76.

14.3. 6-Zone Mode

By default, ESIM364 alarm system runs in the 6-Zone mode under zone connection Type 1 allowing to connect up to 6 detection devices of NO (normally-open) type to the on-board zone terminals as indicated in the wiring diagram of Type 1. Once a different zone connection type is set, the detection device wiring must be done according to the wiring diagram of the associated type. Available zone connection types for the 6-Zone mode:

- **Type 1** – Parallel wiring of NO (normally-open) detection device with 5,6kΩ EOL (end-of-line) resistor.
- **Type 2** – Serial wiring of NC (normally-closed) detection device with 5,6kΩ EOL resistor.
- **Type 3** – Combination of serial and parallel wiring of tamper with 5,6kΩ EOL resistor and NC (normally-closed) detection device with 3,3kΩ EOL resistor.

For zone wiring diagrams of the 6-Zone mode, please refer to **2.3.2. Zone Connection Types**.

Set zone connection type for 6-Zone mode

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ZONE TYPE:6-ZONE M → OK → TYPE 1... 3 → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 39 & number of zone connection type:
39 1 # – Type 1
39 2 # – Type 2
39 3 # – Type 3
Example: *392#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

14.4. ATZ (Advanced Technology Zone) Mode

The ATZ mode is a software-based feature that doubles the number of on-board zones and enables two detection devices to be installed per 1 zone terminal. Once this mode is enabled, the zone connection Type 4 is set automatically. The detection devices must be wired to the on-board zone terminals as indicated in the wiring diagram of the associated zone connection type. Available zone connection types for the ATZ mode:

- **Type 4** – Parallel wiring of 2 NC (normally-closed) detection devices with 5,6kΩ and 3,3kΩ EOL (end-of-line) resistors respectively. 5,6kΩ EOL resistor corresponds to zones ranging from Z1 through Z6, while 3,3kΩ EOL resistor corresponds to zones ranging from Z7 through Z12.
- **Type 5** – Combination of serial and parallel wiring of tamper with 5,6kΩ EOL resistor and 2 NC (normally-closed) detection devices with 5,6kΩ and 3,3kΩ EOL resistors respectively. 5,6kΩ EOL resistor corresponds to zones ranging from Z1 through Z6, while 3,3kΩ EOL resistor corresponds to zones ranging from Z7 through Z12.

For zone wiring diagrams of the ATZ mode, please refer to **2.3.2. Zone Connection Types**.

Enable ATZ mode

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ATZ MODE → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 28 & parameter status value:
28 1 #
Example: *281#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable ATZ mode

EKB2

Menu path:
OK → iiii → OK → ZONES → OK → ATZ MODE → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 28 & parameter status value:
28 0 #
Example: *280#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set zone connection type for ATZ mode

EKB2

Menu path:
OK → CONFIGURATION → OK → iiii → OK → ZONES → OK → ZONE TYPE:ATZ MODE → OK → TYPE 4... 5 → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 38 & number of zone connection type:
381 # – Type 4
382 # – Type 5
Example: *381#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The ATZ mode applies to on-board zones only when enabled.

14.5. Zone Type Definitions

- **Interior Follower** – The zone can be violated during exit and entry delay without causing an alarm. If the zone is violated before the entry delay has begun, it will cause an instant alarm followed by single notification delivery even if the zone has been violated multiple times or another Interrior Follower-type zone has been violated while alarm period (by default - 1 minute) is in progress. The zone is used where violating a zone during exit/entry delay is unavoidable. Typically, this zone is used for indoor protection devices, such as motion detectors, installed close to the exit/entry doors.
- **Instant** – The alarm is instantly caused if this zone is violated when the system is armed or during entry delay. This zone type is usually used for doors, windows or other zones, and shock detectors.
- **24-Hour** – When the system is either armed or disarmed, the zone will cause instant alarm if violated. Normally, this type of zone is used for securing the areas that require constant supervisory.
- **Delay** – This zone type can be violated during exit and entry delay without causing an alarm. If the zone is violated when the system is armed, it will initiate entry delay countdown intended for the user to disarm the system. If the zone is left violated after the exit delay expires, it will cause an instant alarm. If one more zone with Stay-enabled attribute exist and the Delay-type zone is not violated and restored during exit delay, the system will be armed in Stay mode (see **15. STAY MODE**). Typically, this zone type is used for door contacts installed at designated exit/entry doors.
- **Fire** – If this zone type is violated when the system is either armed or disarmed, the alarm will be instantly caused and the siren/bell will emit pulsating sound. Typically, this zone type is used for flame and smoke detectors.
- **Panic/Silent** – This zone operates the same as 24-Hour zone type, but the system will not activate the siren/bell and keypad buzzer if violated. Normally, this zone type used for panic alarm buttons.

Set zone type for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24- HOUR | DELAY | FIRE | PANIC/ SILENT → OK
Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT → OK
Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT → OK
EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 53, zone number & zone type number:
53 nn 1 # – Interior Follower
53 nn 2 # – Instant
53 nn 3 # –24-Hour
53 nn 4 # – Delay
53 nn 5 # – Fire
53 nn 6 # – Panic/Silent
Value: *nn* – zone number, range – [01... 76]
Example: *53125#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The system will NOT activate siren/bell and keypad buzzer only when Panic/Silent zone type is violated.

14.6. Zone Attributes

- **Stay** – If this attribute is enabled, the zone, regardless of type, will not cause an alarm if violated when the system is Stay armed. For more details on arming the system in the Stay mode, please refer to **15. STAY MODE**.
- **Force** – This attribute determines whether the system can be armed or not while a zone is violated. If a zone with the Force attribute enabled is left violated until the exit delay expires, it will be ignored. Once the system is armed and the zone is restored, the violation will not be ignored and the zone will operate according to the determined type. For more details on zone types, please refer to **14.5. Zone Type Definitions**.
- **Shared** – This attribute determines whether a zone, assigned to multiple partitions, will cause an alarm or not in the associated armed partition if violated. If a zone with the Shared attribute enabled is violated when at least one of the associated partitions is disarmed, the alarm will not be caused. Once the system is armed in all of the associated partitions, the zone with Shared attribute enabled will operate according to the determined type. Typically, this attribute is used for shared areas, such as corridors.
- **Delay, ms** – This attribute determines the zone sensitivity level by delay time (By default – 800 milliseconds). If a zone is left triggered until the delay time expires, the zone is considered violated.
- **Delay becomes Instant in Stay mode** – This attribute determines whether or not any Delay type zone will operate as Instant type zone when the system is armed in the Stay mode. When the system is fully armed, the Delay type zone will operate normally. For more details on Delay and Instant zone types, please refer to **14.5. Zone Type Definitions**.
- **Chime** – This feature is used to emit 3 short beeps from the keypad buzzer whenever any Delay type zone is violated while the system is disarmed. Typically, the feature is used for designated exit/entry doors to indicate the opening of the doors.

NOTE: Due to battery power saving reasons, EKB3W wireless keypad buzzer will not sound if the Bell attribute is not enabled and the violated Delay type zone is not of the associated EKB3W wireless keypad. For more details on EKB3W wireless keypad, please refer to **33.2.1. EKB3W - Wireless LED Keypad.**

Enable Stay attribute for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STAY → OK → ENABLE → OK

Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STAY → OK → ENABLE → OK

Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEPAD ZONE → OK → STAY → OK → ENABLE → OK

EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 56, zone number & parameter status value:
56 nn 1 #

Value: *nn* – zone number, range – [01... 76].
Example: *56041#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Stay attribute for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STAY → OK → DISABLE → OK

Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STAY → OK → DISABLE → OK

Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → STAY → OK → DISABLE → OK

EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 56, zone number & parameter status value:
56 nn 0 #
Value: *nn* - zone number, range - [01... 76].
Example: *56190#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Force attribute for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → FORCE → OK → ENABLE → OK

Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → FORCE → OK → ENABLE → OK

Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → FORCE → OK → ENABLE → OK

EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → FORCE → OK → ENABLE → OK

Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 82, zone number & parameter status value:
82 nn 1 #
Value: *nn* - zone number, range - [01... 76].
Example: *82061#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Force attribute for individual zone

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → FORCE → OK → DISABLE → OK

Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → FORCE → OK → DISABLE → OK

Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → FORCE → OK → DISABLE → OK

EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → FORCE → OK → DISABLE → OK

Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 82, zone number & parameter status value:
82 nn 0 #
Value: *nn* - zone number, range - [01... 76].
Example: *82110#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable/disable Shared attribute for individual zone

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set Delay, ms atrribute

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable/disable Delay becomes Instant in Stay mode attribute

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Chime attribute

EKB2
Menu path:
OK →iiii → OK → ZONES → OK → CHIME → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W
Enter parameter 32 & parameter status value:
32 0 #
Example: *320#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Chime attribute

EKB2
Menu path:
OK →iiii → OK → ZONES → OK → CHIME → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W
Enter parameter 32 & parameter status value:
32 1 #
Example: *321#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

14.7. Bypassing and Activating Zones

ATTENTION: Zone bypassing and activation must be carried out without Configuration mode being activated by the EKB3/EKB3W keypad.

Zone bypassing allows the user to deactivate a violated zone and arm the system without restoring the zone. If a bypassed zone is violated or restored during exit/entry delay, or when then system is armed, it will be ignored. When a zone is bypassed, EKB3/EKB3W keypad indicator BYPS will light ON and EKB2 keypad will display ⌂ icon in the home screen view.

Bypass individual violated zone

EKB2
Menu path:
OK → uumm → OK → BYPASS → OK → BYPASS LIST 1... 5 → OK → Z1-zone-name... Z76-zone-name → OK → BYPASS → OK
Value: *uumm* – 4-digit user/master code; *zone-name* – up to 24 characters zone name.

EKB3/ EKB3W
Press the [BYPS[key, enter zone number & user/master code:
BYPS nn uumm #
Value: *nn* – zone number, range – [01... 76]; *uumm* – 4-digit user/master code.
Example: *BYPS091111#*

Bypass all violated zones

EKB2
Menu path:
OK → uumm → OK →BYPASS → OK → BYP VIOLATED ZONES → OK
Value: *uumm* – 4-digit user/master code.

The zone will stay bypassed until the system is disarmed. Once the system is disarmed, the corresponding zone state will be indicated on the keypads (see **32.1.1. EKB2 - LCD Keypad**, **32.1.2. EKB3 - LED Keypad** and **33.1. EKB3W - Wireless LED Keypad**) and Info SMS text message (see **26. SYSTEM INFORMATION. INFO SMS**). Alternatively, the user can activate the bypassed zone by the following configuration methods.

Activate bypassed zone

EKB2

Menu path:
OK → uumm → OK → BYPASS → OK → BYPASS LIST 1... 5 → OK → Z1-zone-name... Z76-zone-name → OK → UNBYPASS → OK
Value: *uumm* - 4-digit user/master code; *zone-name* - up to 24 characters zone name.

EKB3/ EKB3W

Press the [BYPS[key, enter zone number & user/master code:
BYPS nn uumm #
Value: *nn* - zone number, range - [01... 76]; *uumm* - 4-digit user/master code.
Example: *BYPS251111#*

NOTE: Zones can only be bypassed and activated when the system is not armed.

14.8. Zone Names

Each zone has a name that can be customized by the user. Typically, the name specifies a device type connected to a determined zone terminal, for **Example:** Kitchen doors opened. The zone names are used in SMS text messages that are sent to the user during alarm. the By default, the zone names are: *Z1 - Zone1, Z2 - Zone2, Z3 - Zone3, Z4 - Zone4 etc.*

Set zone name

SMS

SMS text message content:
ssss_Znn:zone-name
Value: *ssss* - 4-digit SMS password; *nn* - zone number, range - [1... 76]; *zone-name* - up to 24 characters zone name.
Example: *1111_Z3:Door sensor triggered*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View zone names

SMS

SMS text message content:
ssss_STATUS
Value: *ssss* - 4-digit SMS password.
Example: *1111_STATUS*

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → NAME
Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → NAME
Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → NAME
EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → NAME
Value: *iiii* - 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Colon, semi-colon characters, parameter names and/or values, such as PSW, STATUS, ON, OFF etc. are NOT allowed in zone names

NOTE: Multiple zone names can be set by a single SMS text message, **Example:** *1111_Z1:Kitchen doors opened;Z3:Movement in basement;Z4:Bedroom window opened*

14.9. Disabling and Enabling Zones

By default, all zones, except keypad and virtual zones, are enabled. To permanently disable/enable an individual zone, please refer to the following configuration methods.

Disable zone

SMS

SMS text message content:
ssss_Znn:OFF
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 76].
Example: *1111_Z13:OFF*

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STATUS → OK → DISABLE → OK

Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STATUS → OK → DISABLE → OK

Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → STATUS → DISABLE → OK

EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STATUS → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 52, zone number & parameter status value:
52 nn 0 #
Value: *nn* – zone number, range – [01... 76].
Example: *52360#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable zone

SMS

SMS text message content:
ssss_Znn:ON
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 76].
Example: *1111_Z6:ON*

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STATUS → OK → ENABLE → OK

Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STATUS → OK → ENABLE → OK

Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → STATUS → ENABLE → OK

EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STATUS → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 52, zone number & parameter status value:
52 nn 1 #
Value: *nn* – zone number, range – [01... 76].
Example: *52151#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

15. STAY MODE

Stay mode allows the user to arm and disarm the alarm system without leaving the secured area. If the zones with Stay attribute enabled are violated when the system is Stay armed, no alarm will be caused. Typically, this feature is used when arming the system at home before going to bed.

The system can be Stay armed under the following conditions:

- If a zone with Stay attribute enabled is NOT violated during exit delay, the system will arm in Stay mode. When arming the system in Stay mode under this condition, one of the available arming methods must be used that provide exit delay. For more details on these methods, please refer to **13. EXIT AND ENTRY DELAY.**
- The system will instantly arm in Stay mode when using one of the following methods.

Arm the system in Stay mode

EKB2

Menu path:
Non-partitioned system: P2 → uumm → OK
Partitioned system: P2 → uumm → OK → [p] part-name → OK
Value: *uumm* - 4-digit user/master code; *p* - partition number, range - [1... 4]; *part-name* - up to 15 characters partition name.

EKB3/ EKB3W

Press the [STAY] key & enter user/master:
STAY uumm
Value: *uumm* - 4-digit user/master code.
Example: *STAY1111*

When one or more system partitions are successfully armed in Stay mode, EKB2 keypad will display ⌂ icon in the home screen view.

NOTE for EKB3/EKB3W: System arming in Stay mode by the keypad must be carried out without Configuration mode being activated.

NOTE: The system can be armed in Stay mode, only if there is at least one zone with Stay attribute enabled.

NOTE: Stay mode is not supported by virtual zones.

For more details on how to enable Stay attribute for zone, please refer to **14.6. Zone Attributes**.

16. TAMPERS

The tamper circuit is a single closed loop such that a break in the loop at any point will cause a tamper alarm regardless of the system status – armed or disarmed. During the tamper alarm, the system will activate the siren/bell and the keypad buzzer and send the SMS text message to the preset user phone number. The system will cause tamper alarm under the following conditions:

- If the enclosure of a detection device, siren/bell, metal cabinet or keypad is opened, the physical tamper switch will be triggered. By default, indicated as *Tamper x* in the SMS text message (x = tamper number).
- If the wireless signal is lost due to low signal level or low battery power on a certain wireless device and does not restore during 1 hour period. This event is identified as Wireless Signal Loss. By default, indicated as *No wireless signal from wless-dev wless-id Tamper x* in the SMS text message (*wless-dev* = wireless device model; *wless-id* = 8-digit wireless device ID code; x = tamper number).

By default, tamper alarm notification by SMS text message is enabled. To disable/enable tamper alarm notification, please refer to the following configuration methods.

Disable tamper alarm notification

EKB2

Menu path:
Tamper alarm

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → SMS REPORT → OK → DISABLE → OK

Wireless signal loss

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → SMS REPORT → OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
Tamper alarm

User phone number: 25 13 up 0 #

SMS text message to all users simultaneously: 21 13 up 0 #

SMS delivery report: 55 13 up 0 #

Wireless signal loss

User phone number: 25 18 up 0 #

SMS text message to all users simultaneously: 21 18 up 0 #

SMS delivery report: 55 18 up 0 #

Value: *up* - user phone number slot, range - [01... 10].

Example: *2518031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable tamper alarm notification

EKB2

Menu path:

Tamper alarm

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → SMS REPORT → OK → ENABLE → OK

Wireless signal loss

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → SMS REPORT → OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:

Tamper alarm

User phone number: 25 13 up 1 #

SMS text message to all users simultaneously: 21 13 up 1 #

SMS delivery report: 55 13 up 1 #

Wireless signal loss

User phone number: 25 18 up 1 #

SMS text message to all users simultaneously: 21 18 up 1 #

SMS delivery report: 55 18 up 1 #

Value: *up* - user phone number slot, range - [01... 10].

Example: *2513041#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how to view violated tamper, please refer to **17. ALARM INDICATIONS AND NOTIFICATIONS**

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following feature:

- System arming is blocked if any system fault exists. The user will not be able to arm the system until all existing system faults are solved.
- System arming is blocked until tamper fault is cleared by the installer.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **36. EN 50131-1 GRADE 3.**

16.1. Tamper Names

Each tamper has a name that can be customized by the user. The tamper names are used in SMS text messages that are sent to the user during the tamper alarm. By default, the tamper names are: *Tamper 1, Tamper 2, Tamper 3, Tamper 4 etc*. To set a different tamper name, please refer to the following configuration methods.

Manage tamper name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

17. ALARM INDICATIONS AND NOTIFICATIONS

When a zone, depending on zone type (see **14.5. Zone Type Definitions**), or tamper is violated, the system will cause an alarm. By default, the alarm duration is 1 minute (see **20. SIREN/BELL** regarding the alarm duration). During the alarm, the system will follow this pattern:

1. The system activates the siren/bell and the keypad buzzer.

a) The siren/bell will emit pulsating sound if the violated zone is of Fire type, otherwise the sound will be steady.

b) The keypad buzzer will emit short beeps.

c) EKB2 keypad will display **! ! !** icon next to the alarmed partition in the home screen view followed by 🔊 icon indicating the presence of the alarm events in the alarm log (see **28. EVENT AND ALARM LOG**). In case a Fire-type zone is violated in any system partition, 🔥 icon will appear in the home screen view.

d) EKB3 keypad operating in 4-partition mode will flash the [1]... [4] key corresponding to the alarmed partition number.

e) If one or more zones are violated, EKB3/EKB3W will light ON the corresponding violated zone indicator (-s) ranging from 1 through 12. Indicator SYSTEM will flash if one or more high-numbered zones are violated. If one or tampers are violated, indicator SYSTEM will light ON. For more details on viewing violated high-numbered zone and tamper numbers by EKB3/EKB3W keypad, please refer to **29. INDICATION OF SYSTEM FAULTS**.

2. The system attempts to send an SMS text message, containing the violated zone/tamper name (see **14.8. Zone Names** on how to set a zone name), to the first preset user phone number, sharing the same partition as the violated zone/tamper. The system will send SMS text messages regarding each violated zone/tamper separately.

a) If the user phone number is unavailable and the system fails to receive the SMS delivery report during 20 seconds, it will attempt to send the SMS text message to the next preset user phone number, assigned to the same partition as the previous one. The user phone number may be unavailable due to the following reasons:

- mobile phone was switched off.
- was out of GSM signal coverage.

b) By default, the system will continue sending the SMS text message to the next preset user phone numbers in the priority order until one is available. The system sends the SMS text message only once and will not return to the first user phone number if the last one was unavailable.

3. By default, the system attempts to ring the first user phone number via GSM, sharing the same partition as the violated zone/tamper. The system will dial regarding each violated zone/tamper separately.

a) When the call is answered, the system will shut down the siren/bell and play the audio file that can be listened to on the user's mobile phone. This feature will be available only if an audio file is recorded and assigned to the violated zone (see **17.2. Audio Files**).

b) When the audio record has played, the user will be able to listen on the mobile phone for approx. 30 seconds to what is happening in the area, surrounding the alarm system. This feature will be available only if a microphone is connected to the system (see **25. REMOTE LISTENING AND 2-WAY VOICE COMMUNICATION**).

c) The system will dial the next preset user phone number, assigned to the same partition, if the previous user was unavailable due to the following reasons:
- mobile phone was switched off.
- mobile phone was out of GSM signal coverage.
- provided "busy" signal.
- user did not answer the call after several rings, predetermined by the GSM operator.

d) The system will continue dialing the next preset user phone numbers in the priority order until one is available. The system will dial the user phone number 5 times if the first user phone number was out of GSM signal coverage/switched OFF, otherwise the system will dial only once. If the system ends up with all unsuccessful to contact any preset user phone number, will stop dialing and will not return to the first user phone number.

e) The system will not dial the next preset user phone number if the previous one was available, but rejected the phone call.

4. If enabled, the system attempts to ring the first phone number via PSTN (see **30.2.3. PSTN**). The system will dial regarding each violated zone/tamper separately.

a) When the call is answered, the system will automatically drop the call.

b) The system will dial the next preset phone number if the previous one was unavailable due to the following reasons:
- mobile phone was switched off.
- mobile phone was out of GSM signal coverage.
- provided "busy" signal.
- user did not answer the call after several rings, predetermined by the GSM operator.

c) The system will continue dialing the next preset phone numbers in the priority order until one is available. The system will dial the phone number 5 times (by default) if the first phone number was unavailable. If the system ends up with all unsuccessful to contact any preset phone number, it will return to the first phone number.

To silent the siren/bell as well as to cease system phone calls and SMS text message sending to the user phone numbers, please disarm the system (see **12. ARMING AND DISARMING**).

ATTENTION: The wireless siren EWS1/EWS2/EWS3 will sound only if wireless zone of the siren is assigned to the same partition as the one that has been alarmed (see **23.1. Zone Partition**).

View violated zones

SMS

SMS text message content:
ssss_INFO
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO*

EKB2

Menu path:
OK → uumm → OK → VIOLATED ZONES → OK → ZONE 1... 76
Value: *uumm* – 4-digit user/master code.

EKB3/ EKB3W

Please, refer to illuminated zone indicators ranging from 1 through 12 on the keypad. The flashing indicator SYSTEM stands for violated high-numbered zones (Z13-Z76). For more details on violated high-numbered zone indication, please refer to **29. INDICATION OF SYSTEM FAULTS.**

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View violated tampers

SMS

The systemwill automatically send an SMS text message, containing a violated tamper name, to user phone number.

EKB2

Menu path:
OK → uumm → OK → VIOLATED TAMPERS → OK → TAMPER 1... 76
Value: *uumm* – 4-digit user/master code.

EKB3/ EKB3W

The illuminated indicator SYSTEM stands for system fault presence including violated tamper. For more details on violated tamper indication, please refer to **29. INDICATION OF SYSTEM FAULTS.**

For more details details on how to disable/enable SMS text messages and phone calls to preset user phone number in case of alarm, please refer to **17.1. Enabling and Disabling Alarm Notifications**

ATTENTION: Phone calls to the preset user phone number in case of alarm are disabled by force when MS mode is enabled (see **30. Monitoring Station**).

NOTE: If one or more zones/tampers are violated during the alarm, the system will attempt to send as many SMS text message and dial the user phone number as many times as the zone/tamper was violated.

NOTE: If the system sent the SMS text message and/or dialed the user phone number after disarming the system, it means that the SMS text message and/or phone call was queued up in the memory before the system was disarmed

17.1. Enabling and Disabling Alarm Notifications

By, default the system will ring the preset user phone numbers via GSM in case of alarm. To disable/enable this feature, please refer to the following configuration methods.

Disable call in case of alarm

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CALL IN CASE ALARM → OK → GSM USER 1... 10 → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 30, user phone number slot & parameter status value:
30 us 1 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *30081#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable call in case of alarm

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CALL IN CASE ALARM → OK → GSM USER 1... 10 → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 30, user phone number slot & parameter status value:
30 us 0 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *30090#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By, default the system will send SMS text message to preset user phone numbers in case of alarm. To disable/enable this feature, please refer to the following configuration methods.

Disable SMS text message in case of alarm

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → SMS REPORT → OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 03 up 0 #

SMS text message to all users simultaneously: 21 03 up 0 #

SMS delivery report: 55 03 up 0 #

Value: *up* - user phone number slot, range - [01... 10].
Example: *2503060#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable SMS text message in case of alarm

EKB2

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → SMS REPORT → OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 03 up 1 #

SMS text message to all users simultaneously: 21 03 up 1 #

SMS delivery report: 55 03 up 1 #

Value: *up* - user phone number slot, range - [01... 10].
Example: *2503101#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By, default the system will not ring the preset phone number via PSTN in case of alarm. To manage this feature, please refer to **30.2.3. PSTN)**

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

By default, tamper alarm notification by SMS text message is enabled. For more details on how to disable/enable tamper alarm notification, please refer to **16. TAMPERS**.

ATTENTION: Regardles of the Call in Case of Alarm parameter status, the system will NOT ring the preset user phone number via GSM if the system is connected to the monitoring station (see **30. MONITORING STATION**) and/or when Smart Security feature is in use (see **37. SMART SECURITY**).

17.2. Audio Files

The system comes equipped with a feature allowing to record up to 16 audio files of up to 6 seconds length using the microphone of the PC. The recorded file can be assigned to any system zone, except virtual zone, and be played when the alarm is caused by zone with an audio file assigned. This feature will be available only if the system is able to dial user phone number in the event of an alarm and the user answers the call. The supported audio file format is as follows:

- Max. number of audio files: up to 16
- Max. audio length: up to 6 seconds
- File format: .wav
- Specifications: 8,000 kHz; 8 Bit; Mono

Record and manage audio files

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Assign audio file to individual zone

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Single audio file can be assigned to multiple zones.

18. PROGRAMMABLE (PGM) OUTPUTS

A PGM output is a programmable output that toggles to its set up state when a specific event has occurred in the system, the scheduled weekday and time has come or if the user has initiated the PGM output state change manually. Normally, PGM outputs can be used to open/close garage doors, activate lights, heating, watering and much more. When a PGM output turns ON, the system triggers any device or relay connected to it.

ESIM364 comes equipped with four open-collector PGM outputs allowing to connect up to four devices or relays. For more details on PGM output expanding, please refer to **18.2. PGM Output Expansion**.

ESIM364 PGM outputs are classified by 4 categories:

PGM output category	Description	Max. number of PGM outputs per device	Max. number of PGM outputs in total
On-board PGM Outputs	Built-in wired PGM outputs of ESIM364 alarm system.	4	4
EPGM8 PGM Outputs	PGM outputs of EPGM8 - hardwired PGM output expansion module.	8	8
EPGM1 PGM Outputs	PGM outputs of EPGM1 - hardwired zone & PGM output expansion module.	2	4
Wireless PGM Outputs	Non-physical PGM outputs automatically created by connected wireless devices.	2*	64**

* - Depends on the connected wireless device.
** - Available only if no EPGM1 PGM outputs are present.

For PGM output wiring diagram, please refer to **2.3.6. Relay Finder® 40.61.9.12 with Terminal Socket 95.85.3**.

18.1. PGM Output Numbering

The PGM output numbers ranging from C1 through C12 are permanently reserved for on-board PGM outputs even if EPGM8 module mode is disabled. The C13-C76 PGM output number are automatically assigned in the chronological order to the devices connected to the system: EPGM1 modules and wireless devices.

18.2. PGM Output Expansion

For additional electrical appliance connection, the number of PGM outputs can be expanded by:

- connecting EPGM8 hardwired PGM output expansion module. (see **18.2.1. EPGM8 Mode and 32.3.1. EPGM8 - Hardwired PGM Output Expansion Module**)
- connecting EPGM1 hardwired zone and PGM output expansion module (see **32.1.3. EPGM1 - Hardwired Zone & PGM Output Expansion Module**).
- binding the wireless devices (see **19. WIRELESS DEVICES**).

The maximum supported PGM output number is 76.

18.2.1. EPGM8 Mode

EPGM8 is an expansion module, which expands the system with 8 additional hardwired PGM outputs. For more details on EPGM8 module installation, please refer to **32.3.1. EPGM8 - Hardwired PGM Output Expansion Module**.

Once the EPGM8 module is installed, the EPGM8 mode must be enabled.

Enable EPGM8 mode

EKB2

Menu path:
OK → iiii → OK → PGM OUTPUTS → OK → USING EPGM8 → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/EKB3W

Enter parameter 33 & parameter status value:
33 1 #
Example: *331#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable EPGM8 mode

EKB2

Menu path:
OK → iiii → OK → PGM OUTPUTS → OK → USING EPGM8 → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 33 & parameter status value:
33 0 #
Example: *330#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

18.3. PGM Output Names

Each PGM output has a name that can be customized by the user. Typically, the name specifies a device type connected to a determined PGM output, for **Example:** Lights. The name can be used instead of PGM output number when controlling the PGM output by SMS text message. By default, the PGM output names are: *C1 – Controll1, C2 – Controll2, C3 – Controll3, C4 – Controll4 etc.*

Set PGM output name

SMS

SMS text message content:
ssss_Coo:out-name
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name.
Example: *1111_C2:Lights*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View PGM output names

SMS

SMS text message content:
ssss_STATUS
Value: *ssss* – 4-digit SMS password.
Example: *1111_STATUS*

EKB2

Menu path:
On-board PGM output: OK → iiii → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → NAME
Wireless PGM output: OK → iiii → OK → PGM OUTPUTS → OK → WIRELESS OUTPUTS 1... 4 → OK → OUTPUT 13... 76 → OK → NAME
Value: *iiii* – 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Space, colon, semi-colon characters, parameter names and/or values, such as PSW, STATUS, ON, OFF etc. are NOT allowed in PGM output names.

18.4. Turning PGM Outputs ON and OFF

By default, all PGM outputs are turned OFF. To instantly turn ON/OFF an individual PGM output and set its state to ON/OFF when the system starts-up, please refer to the following configuration methods.

Turn ON PGM output/ Set PGM output start-up state as ON

SMS

SMS text message content:
ssss_Coo:ON or ssss_out-name:ON
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name.
Example: *1111_Lights:ON*

EKB2

Menu path:
On-board PGM output: OK → iiii → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → STATUS → OK → ENABLE → OK
Wireless PGM output: OK → iiii → OK → PGM OUTPUTS → OK → WIRELESS OUTPUTS 1... 4 → OK → OUTPUT 13... 76 → OK → STATUS → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 61, PGM output number & parameter status value:
61 oo 1 #
Value: *oo* – PGM output number, range – [01... 76].
Example: *61031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

EWK1/ EWK2/ EWK2A

This operation may be carried out from the wireless keyfob if pre-configured using the PC running *ELDES Configuration Tool* software.

Turn OFF PGM output/ Set PGM output start-up state as OFF

SMS

SMS text message content:
ssss_Coo:OFF or ssss_out-name:OFF
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name.
Example: *1111_C2:OFF*

EKB2

Menu path:
On-board PGM output: OK → iiii → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → STATUS → OK → DISABLE → OK
Wireless PGM output: OK → iiii → OK → PGM OUTPUTS → OK → WIRELESS OUTPUTS 1... 4 → OK → OUTPUT 13... 76 → OK → STATUS → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 61, PGM output number & parameter status value:
61 oo 0 #
Value: *oo* – PGM output number, range – [01... 76].
Example: *61020#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

EWK1/ EWK2/ EWK2A

This operation may be carried out from the wireless keyfob if pre-configured using the PC running *ELDES Configuration Tool* software.

To instantly turn ON an individual PGM output for a determined time period and automatically turn it OFF when the time period expires, please refer to the following configuration method.

Turn ON PGM output for time period

SMS

SMS text message content:
ssss_Coo:ON:hr.mm.sc or ssss_out-name:ON:hr.mn.sc
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59]; *sc* – seconds, range – [00... 59].
Example: *1111_C4:ON:10.15.35*

To instantly turn OFF an individual PGM output for a determined time period and automatically turn it ON when the time period expires, please refer to the following configuration method.

Turn OFF PGM output for time period

SMS

SMS text message content:
ssss_Coo:OFF:00.00.sc or ssss_out-name:OFF:hr.mn.sc
Value: *ssss* – 4-digit SMS password;*oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59]; *sc* – seconds, range – [00... 59].
Example: *1111_Lights:OFF:00.00.23*

When the PGM output is turned ON or OFF, the system will send a confirmation by SMS text message to the user phone number that the SMS text message was sent from.

NOTE: PGM output can be turned ON for a determined time period only when it is in OFF state

NOTE: PGM output can be turned OFF for a determined time period only when it is in ON state

NOTE: Multiple PGM outputs can be turned ON/OFF by a single SMS text message, **Example:** *1111_C1:ON C2:OFF Pump:ON C4:ON:00.20.25*

18.5. PGM Output Control by Event and Scheduler

The PGM outputs can automatically operate when a specific event occurs in the system and/or when the scheduled weekday and time comes.

PGM Output Actions

The automatic action of the determined PGM output can be set as follows:

- **Turn ON** – Determines whether the PGM output is to be turned ON.
- **Turn OFF** – Determines whether the PGM output is to be turned OFF.
- **Pulse** – Determines whether the PGM output is to be turned ON for a set period of time in seconds.

System Events

The aforementioned PGM output action can be automatically carried out under the following events that have occurred in the system:

- **System armed** – System is armed in a determined partition ranging from Partition 1 through 4 or any partition.
- **System disarmed** – System is disarmed in a determined partition ranging from Partition 1 through 4 or any partition.
- **Alarm begins** – Alarm begins in a determined partition ranging from Partition 1 through 4 or any partition.
- **Alarm stops** – Alarm stops in a determined partition ranging from Partition 1 through 4 or any partition.
- **Temperature falls** – Temperature falls below the set MIN value of a determined temperature sensor 1-8.
- **Temperature rises** – Temperature rises above the set MAX value of a determined temperature sensor 1-8.
- **Zone violated** – A determined zone ranging from Z1 through Z76 is violated.
- **Zone restored** – A determined zone ranging from Z1 through Z76 is restored.
- **Scheduler starts** – Determines Start Time of a selected scheduler 1-16.
- **Scheduler ends** – Determines End Time of a selected scheduler 1-16.

The user can also set a custom text, which will be sent by SMS text message to user phone number when the automatic PGM output action is carried out.

Schedulers

The system supports up to 16 schedulers that allow the PGM outputs to operate according to the day of the week and time. When the scheduler, which includes the set weekday and time, is selected, the PGM output will operate according to it. Each scheduler includes the following parameters:

- **Always** – The scheduler is not in use.
- **At specified time** – Determines whether weekday and time settings are enabled:
  - **Start Time** – Determines the point in time when the PGM output action can begin.
  - **End Time** – Determines the point in time when the PGM output action can complete.
  - **On weekdays** – Determines days in week when the PGM output action is valid.

Additional Conditions

Additional condition narrows down the chances for a determined automatic PGM output operation to be carried out. If this feature is enabled, the PGM output will become dependent on one more system event that must be occurred prior or must occur after the aforementioned system event. The PGM output will not operate until the chain of system events meets the set values:

- **System armed** – System is armed in a determined partition ranging from 1 to 4 or any partition.
- **System disarmed** – System is disarmed in a determined partition ranging from 1 to 4 or any partition.
- **Zone violated** – A determined zone ranging from Z1 to 76 is violated.
- **Zone restored** – A determined zone ranging from Z1 to Z76 is restored.

Example: *PGM output C1 is set to be turned ON when zone Z6 is violated. The additional condition feature is enabled and set to allow this action to be carried out only if system's Partition 2 is disarmed. It means that the PGM output C1 will be turned ON when zone Z6 is violated, but only if system's Partition 2 is disarmed.*

Manage PGM output control by event & scheduler

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: When both - a system event is determined and a scheduler is selected, the PGM output will operate only if the determined event has occurred in the system during the scheduled time period.

ATTENTION: If the date and time are not set, the system will NOT be able to automatically control the PGM outputs. For more details on how to set date and time, please refer to **9. DATE AND TIME**.

18.6. Wireless PGM Output Type Definitions

- **Output** – Operates as normal PGM output that can be controlled by the user or automatically by event and scheduler. Normally, this type is used for any device or relay.
- **Siren** – Operates as siren output that automatically activates during alarm. Typically, this type is used for bell/siren connected to EW1 wireless device.

Set output type for individual wireless PGM output

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

19. WIRELESS DEVICES

ESIM364 system has a built-in wireless module for system extension capabilities. The wireless module easily allows the user to bind up to 32 ELDES-made wireless devices to the system. This includes the following:

- EWP1 – wireless PIR sensor (motion detector).
- EWD1 – wireless magnetic door contact.
- EWD2 - magnetic door contact/shock sensor
- EWS1 and EWS3 – wireless indoor sirens.
- EWS2 – wireless outdoor siren.
- EWK1 and EWK2 – wireless keyfobs.
- EKB3W – wireless keypad.
- EW1 – wireless zone and PGM output expansion module.
- EW1B – wireless battery-powered zone and PGM output expansion module.
- EWF1 - wireless smoke detector.

The wireless devices can operate at a range of up to 30 meters from the alarm system unit while inside the building and at up to 150 meters range in open areas. The wireless connection is two-way and operates in one of four available channels at 868 Mhz (EU version) / 915 Mhz (US version) non-licensed frequency range. The communication link between the wireless device and the alarm system is constantly supervised by a configurable self-test period, identified as Test Time.

For more details on how to install the wireless devices, please refer to **33. ELDES WIRELESS DEVICES** and **RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION** manual located at www.eldes.lt/download

19.1. Binding, Removing and Replacing Wireless Devicess

When the wireless device is switched ON, it will initiate the data transmission to the system within its wireless connection range. In order to optimize battery power saving of the wireless device, the data transmission periods vary by itself while the device is switched ON, but still unbound. The data transmission period from the system wireless devices when the alarm system is switched OFF or if the wireless device is unbound or removed is as follows:

- EKB3W, EW1, EW1B, EWP1, EWS1, EWS2, EWS3, EWF1:
    - First 360 attempts after the device startup (reset) - every 10 seconds.
    - The rest of attempts - every 1 minute.
- EWD1, EWD2:
    - First 360 attempts after the device startup (reset) - every 10 seconds.
    - The rest of attempts - every 2 minutes.

Once the wireless device is bound, it will attempt to exchange data with ESIM364 system. Due to battery saving reasons, all ELDES wireless devices operate in sleep mode. The data exchange will occur instantly if the wireless device is triggered (zone alarm or tamper alarm) or periodically when the wireless device wakes up to transmit the supervision signal, identified as Test Time, to the system as well as to accept the queued up command (if any) from the system. **Example:** *The alarm occurred at 09:15:25 and the system queued up the command for EWS2 siren to start sounding. By default, Test Time value of EWS2 siren is 7 seconds, therefore EWS2 siren will sound at 09:15:32.*

By default, the Test Time period is as follows:

- EKB3W, EWD1: every 60 seconds.
- EW1, EWP1, EWF1, EWD2: every 30 seconds.
- EW1B: every 20 seconds.
- EWS1, EWS2, EWS3: every 7 seconds.

To set a different Test Time value, please refer to the following configuration method.

Set Test Time

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Test Time affects the wireless device binding process due to the alarm system listening for the incoming data from the wireless device. The system binds the wireless device only when the first data packet is received.

NOTE FOR EKB3W: In comparison with other ELDES wireless devices, EKB3W keypad features some exceptions regarding the wireless communication. For more details on EKB3W keypad wireless communication and back-light timeout, please refer to **33.1.7. Wireless Communication, Sleep Mode and Back-light Timeout.**

An 8-digit wireless device ID code will be required in order to bind the device to the system or to remove it from the system. The wireless ID code is printed on a label, which can be located on the inner or outer side of the enclosure or on the printed circuit board (PCB) of the wireless device.

To bind a wireless device, please refer to the following configuration methods.

Bind wireless device to the system

SMS

SMS text message content:
ssss_SET:wless-id
Value: *ssss* – 4-digit SMS password; *wless-id* – 8-digit wireless device ID code.
Example: *1111_SET:535185D*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE FOR EWK1/EWK2/EKB3W: When binding EWK1/EWK2 wireless keyfob or EKB3W wireless keypad, it is necessary to press several times any button/key on the device.

Once a wireless device is bound, it occupies one of 32 available wireless device slots and the system adds one or two wireless zones and wireless PGM outputs depending on the wireless device model.

To remove a wireless device, please refer to the following configuration methods.

Remove wireless device from the system

SMS

SMS text message content:
ssss_DEL:wless-id
Value: *ssss* – 4-digit SMS password; *wless-id* – 8-digit wireless device ID code.
Example: *1111_DEL:535185D*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Once a wireless device is removed from the system, please restore its default parameters and remove the batteries from it.

To replace an existing wireless device with a new same model device, please refer to the following configuration methods

Replace wireless device

SMS

SMS text message content:
ssss_REP:wless-id<oldwl-id
Value: *ssss* – 4-digit SMS password; *wless-id* – 8-digit wireless device ID code of the old device; *oldwl-id* - 8-digit wireless device ID code of the new device.
Example: *1111_REP:535185D<41286652*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

When a wireless device is successfully replaced with a new one, the configuration of the old wireless device remains.

NOTE: If you are unable to bind a wireless device, please restore the wireless device's parameters to default and try again. For more details on how to restore the default parameters, please refer to the user manual provided along with the wireless device or visit www.eldes.lt/en/download to download the latest user manual

ATTENTION: In order to correctly remove the wireless device from the system, the user must remove the device using SMS text message or *ELDES Configuration Tool* software and restore the parameters of the wireless device to default afterwards. If only one of these actions is carried out, the wireless device and the system will attempt to exchange data to keep the wireless connection alive. This leads to fast battery power drain on the battery-powered wireless device.

19.2. Wireless Device Information and Signal Status Monitoring

Once a wireless device is bound, the user can view the following information of a determined wireless device:

- Battery level (expressed in percentage).
- Wireless signal strength (expressed in percentage).
- Error rate (number of failed data transmission attempts in 10-minute period) - indicated only in EKB2 keypad menu.
- Firmware version.
- Test Time period (expressed in milliseconds) - indicated only in SMS text message reply.

To view the wireless device information, please refer to the following configuration methods.

View wireless device information

SMS

SMS text message content:
ssss_RFINFO:wless-id or ssss_RFINFO:Znn
Value: *wless-id* – 8-digit wireless device ID code; *nn* – wireless zone number, range – [13... 76].
Example: *1111_RFINFO:535185D*

EKB2

Menu path:
Battery level: OK → iiii → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → BATTERY
Wireless signal: OK → iiii → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → SIGNAL
Error rate: OK → iiii → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → ERROR RATE
Firmware version: OK → iiii → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → FW RELEASE
Value: *iiii* – 4-digit installer code; *wless-dev* – wireless device model; *wless-id* – 8-digit wireless device ID code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The system supports up to 32 wireless devices. To view the number of unoccupied wireless device slots in the system, please refer to the following configuration methods

View unoccupied wireless device slots

SMS

SMS text message content:
ssss_STATUS_FREE
Example: *1111_STATUS_FREE*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

When the wireless signal between the system and a wireless device is lost and does not restore during 1 hour period, the system will send notification by SMS text message to preset user phone number. By default, the notification regarding the wireless signal status is enabled. To disable/enable this notification, please refer to **16. TAMPERS.**

19.3. Disabling and Enabling Siren if Wireless Signal is Lost

If a wireless device loses its wireless signal for 1 hour or longer, the system will send notification by SMS text message to user phone number and activate the siren/bell. By default, the siren will not be activated when wireless signal is lost. To enable/disable this feature, please refer to the following configuration methods.

Enable Siren if Wireless Signal is Lost

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS →OK → SRN IF WLESS LOSS → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 76 & parameter status value:
76 1 #
Example: *761#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Siren if Wireless Signal is Lost

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS →OK → SRN IF WLESS LOSS → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 76 & parameter status value:
76 0 #
Example: *760#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

20. SIREN/BELL

When the system is in alarm state, the siren/bell will sound until the set time (By default – 1 minute) expires or until the system is disarmed. To set the alarm duration, please refer to the following configuration methods.

Set alarm duration

SMS

SMS text message content:
ssss_SIREN:t
Value: *ssss* – 4-digit SMS password; *t* – alarm duration, range – [0... 5] minutes.
Example: *1111_SIREN:4*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → ALARM DURATION → OK → tt → OK
Value: *iiii* – 4-digit installer code; *tt* – alarm duration, range – [1... 10] minutes.

EKB3/ EKB3W

Enter parameter 10 & alarm duration:
10 tt #
Value: *tt* – alarm duration, range – [00... 10] minutes.
Example: *1007#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View alarm duration

SMS

SMS text message content:
ssss_SIREN
Value: *ssss* – 4-digit SMS password
Example: *1111_SIREN*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → ALARM DURATION
Value: *iiii* – 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For siren/bell wiring diagram, please refer to **2.3.3. Siren**.

NOTE: 0 value disables the siren/bell.

NOTE: Due to battery power saving reasons, the wireless siren will sound for 1 minute regardless of the set alarm duration time, unless it is set to 0.

20.1. BELL Output Status Monitoring

The system constantly supervises the BELL output. If the siren/bell is disconnected/cut-off, the system will instantly send the notification by SMS text message to User 1 and indicate system fault condition on the keypad (see **29. INDICATION OF SYSTEM FAULTS**). Once the bell/siren is connected/fixed, the system will notify User 1 by SMS text message and the keypad will no longer indicate system fault.

By default, the notification by SMS text message regarding the BELL output status is disabled. To enable/disable this notification, please refer to the following configuration methods.

Enable Siren Fail/ Restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → SMS TO ALL → OK → ENABLE → OK
MS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → SMS REPORT → OK → ENABLE → O
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 08 up 1 #
SMS text message to all users simultaneously: 21 08 up 1 #
SMS delivery report: 55 08 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2508021#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Siren Fail/ Restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 08 up 0 #
SMS text message to all users simultaneously: 21 08 up 0 #
SMS delivery report: 55 08 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2508040#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

20.2. Bell Squawk

If enabled, the siren/bell indicates the completed system arming and disarming process. After the system is successfully armed, the siren/bell will emit 2 short beeps and 1 long beep after the system is disarmed. To enable/disable the Bell Squawk feature, please refer to the following configuration methods.

Enable Bell Squawk

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 29 & parameter status value:
291 #
Example: *291#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Bell Squawk

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 29 & parameter statusvalue:
290 #
Example: *290#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

20.3. Bell Squawk in Stay Mode

If enabled, the Bell Squawk will be available when arming/disarming the system in Stay mode (see **15. STAY MODE**). To enable/disable this feature, please refer to the following configuration methods

Enable Bell Squawk in Stay Mode

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK STAY → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 95 & parameter status value:
951 #
Value: *951#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

Disable Bell Squawk in Stay Mode

EKB2	**Menu path:** OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK STAY → OK → DISABLE → OK **Value:** *iiii* – 4-digit installer code.
EKB3/ EKB3W	**Enter parameter 95 & parameter status value:** 95 0 # **Value:** *950#*
Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

20.4. Indication by EWS2 Indicators

When enabled, the built-in LED indicators of EWS2 wireless outdoor siren will flash during the alarm. To enable/disable this feature, please refer to the following configuration methods.

Enable EWS2 LED indication

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS2 LED → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 29 & parameter status value:
88 1 #
Example: *881#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable EWS2 LED indication

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS2 LED → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 29 & parameter status value:
88 0 #
Example: *880#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

20.5. Indication by EWS3 Indicators

When enabled, the built-in LED indicators of EWS3 wireless indoor siren will flash during the alarm. In the event of burglary, 24-hour or tamper alarm, EWS3 will flash the blue LED indicators, while in case of a fire alarm, the device can flash the red LED indicator. To enable/disable these features, please refer to the following configuration methods.

Enable EWS3 LED indication

EKB2

Menu path:
Burglary/24-hour/tamper alarm LED: OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS3 ALARM LED → OK → ENABLE → OK
Fire alarm LED: OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS3 FIRE LED → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 94/93 & parameter status value:
Burglary/24-hour/tamper alarm LED: 93 1 #
Fire alarm LED: 93 1 #
Example: *931#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software.*

Disable EWS3 LED indication

EKB2

Menu path:
Burglary/24-hour/tamper alarm LED: OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS3 ALARM → OK → DISABLE → OK
Fire alarm LED: OK → iiii → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS3 FIRE LED → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 94/93 & parameter status value:
Burglary/24-hour/tamper alarm LED: 93 0 #
Fire alarm LED: 93 0 #
Example: *940#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

20.6. EWF1 Interconnection

The interconnection feature automatically links all wireless smoke detectors to each other that are connected to the same alarm system unit. When any EWF1 detects smoke, it sounds the alarm and sends the signal to the alarm system that causes an instant alarm along with the rest of EWF1 wireless smoke detectors. The device that detected smoke will auto-reset when the smoke clears, while the rest of EWF1 detectors will sound in accordance with the set time period (by default - 30 seconds).

By default, the interconnection feature is enabled and the siren alarm duration is 30 seconds. To manage these parameters, please refer to the following configuraiton methods.

Disable interconnection

EKB2 **Menu path:**
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWF1 SIREN INTERC. → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W **Enter parameter 50 & parameter status value:**
50 0 #
Example: *500#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable interconnection

EKB2 **Menu path:**
OK → iiii → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWF1 SIREN INTERC. → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W **Enter parameter 29 & parameter status value:**
50 1 #
Example: *501#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set EWF1 siren alarm duration

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on EWF1 wireless smoke detector, please refer to **33.9. EWF1 - Wireless Smoke Detector**

21. BACKUP BATTERY, MAINS POWER SUPPLY STATUS MONITORING AND MEMORY

The system may come equipped with a backup battery maintaining power supply of the system when the mains power supply is temporally lost. The implemented feature allows the system to perform a self-test on the backup battery and notify User 1 by SMS text message as well as to indicate system fault by the keypad (see **29. INDICATION OF SYSTEM FAULTS**) if:

- battery has failed and requires replacement – battery resistance is 2Ω or higher; self-tested every 24 hours.
- battery is dead or missing – battery is not present or battery voltage is below 5V; self-tested every 1 minute.
- battery power is running low – battery voltage is 10.5V or lower; constantly self-tested.

By default, all notifications regarding the backup battery status are enabled. To disable/enable a determined backup battery notification, please refer to the following configuration methods.

Disable Battery Failed notification

EKB2

Menu path:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → SMS REPORT → OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:

User phone number: 25 05 up 0 #

SMS text message to all users simultaneously: 21 05 up 0 #

SMS delivery report: 55 05 up 0 #

Value: *up* - user phone number slot, range - [01... 10].

Example: *2105010#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Battery Failed notification

EKB2

Menu path:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → SMS REPORT → OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:

User phone number: 25 05 up 1 #

SMS text message to all users simultaneously: 21 05 up 1 #

SMS delivery report: 55 05 up 1 #

Value: *up* - user phone number slot, range - [01... 10].

Example: *2505031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Battery Dead or Missing notification

EKB2

Menu path:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → SMS REPORT → OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 06 up 0 #
SMS text message to all users simultaneously: 21 06 up 0 #
SMS delivery report: 55 06 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *5506070#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Battery Dead or Missing notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 06 up 1 #
SMS text message to all users simultaneously: 21 06 up 1 #
SMS delivery report: 55 06 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *5506101#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Low Battery notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 07 up 0 #
SMS text message to all users simultaneously: 21 07 up 0 #
SMS delivery report: 55 07 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2107100#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Low Battery notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 07 up 1 #
SMS text message to all users simultaneously: 21 07 up 1 #
SMS delivery report: 55 07 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2107021#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If the household electricity is unstable in the system installation area, the system may temporally lose its power supply and continue operating on the backup battery power. The system supervises the mains power supply and notifies User 1 by SMS text message as well as indicates system fault condition on the keypad (see **29. INDICATION OF SYSTEM FAULTS**) when the mains power is lost. When the mains power restores, the system will notify User 1 by SMS text message and the keypad will no longer indicate system fault.

By default, system notification by SMS text message regarding mains power supply status is enabled. To disable/enable this notification, please refer to the following configuration methods.

Disable mains power supply loss/restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R → OK → GSM USER 1... 10 → OK → DISBLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 04 us 0 #
SMS text message to all users simultaneously: 21 04 us 0 #
SMS delivery report: 55 04 us 0 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *2504050#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable mains power supply loss/restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 04 up 1 #
SMS text message to all users simultaneously: 21 04 up 1 #
SMS delivery report: 55 04 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2514091#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, mains power supply loss and restore delay are 30 and 120 seconds respectively. To set a different mains power supply loss and restore delay duration, please refer to the following configuration methods.

Set mains power supply loss delay

EKB2

Menu path:
OK → iii → OK → PRIMARY SETTINGS → OK → MAIN POWER STATUS → OK → LOSS DELAY → OK → lllll → OK

Value: *iiii* – 4-digit installer code; *lllll* – mains power loss delay duration, range - [0... 65535] seconds.

EKB3/ EKB3W

Enter parameter 70 & loss delay duration:
70 lllll #

Value: *lllll* – mains power loss delay duration, range - [0... 65535] seconds.
Example: *7043#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set mains power supply restore delay

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → MAIN POWER STATUS → OK → RESTORE DELAY → OK → rrrrr → OK

Value: *iiii* – 4-digit installer code; *w* – mains power restore delay duration, range - [0... 65535] seconds.

EKB3/ EKB3W

Enter parameter 71 & restore delay duration:
71 rrrrr #

Value: *rrrrr* – mains power restore delay duration, range - [0... 65535] seconds.
Example: *71150#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The configuration settings and event log records are stored in a built-in EEPROM memory, therefore even if the system is fully shut down, the configuration and event log remain. For more details regarding the event log, please refer to **28. EVENT AND ALARM LOG.**

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

NOTE: In order to view the backup battery voltage, resistance, mains power supply status and value, please refer to Diagnostic Management feature available on *ELDES Configuration Tool* software.

22. GSM CONNECTION AND ANTENNA STATUS MONITORING

The system supervises the GSM connection every 10 minutes. When the GSM signal is lost, the system indicator NETW will light OFF, the GSM modem automatically restarts, the keypad will indicate system fault condition (see **29. INDICATION OF SYSTEM FAULTS**) and the system will turn ON a determined PGM output if the GSM signal is lost for a longer time period than the set delay value (By default – 180 seconds). Once the GSM signal restores, the system will notify User 1 by SMS text message, the keypad will no longer indicate system fault and the determined PGM output will turn OFF.

By default, the notifications by SMS text message regarding GSM signal loss is disabled. To enable/disable thus notification, please refer to the following configuration methods.

Enable GSM Connection Failed notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → GSM USER 1... 10 → OK → ENABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → SMS TO ALL → OK → ENABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → SMS REPORT → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 11 up 1 #
SMS text message to all users simultaneously: 21 11 up 1 #
SMS delivery report: 55 11 up 1 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2114091#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable GSM Connection Failed notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → GSM USER 1... 10 → OK → DISABLE → OK
SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → SMS TO ALL → OK → DISABLE → OK
SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → SMS REPORT → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 11 up 0 #
SMS text message to all users simultaneously: 21 11 up 0 #
SMS delivery report: 55 11 up 0 #
Value: *up* - user phone number slot, range - [01... 10].
Example: *2114020#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, the PGM output for GSM signal loss indication is not set. To set the PGM output and delay duration for GSM signal loss indication, please refer to the following configuration method.

Manage GSM signal loss indication by PGM output

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The system constantly monitors the GSM/GPRS antenna status. If the GSM/GPRS antenna is disconnected/cut-off, the system will send notification by SMS text message to User 1 and the keypad will indicate system fault condition (see **29. INDICATION OF SYSTEM FAULTS**) . Once the antenna is connected/fixed, the system will notify User 1 by SMS text message and the keypad will no longer indicate system fault.

By default, the notification by SMS text message regarding the GSM/GPRS antenna status is disabled. To enable/disable this notification, please refer to the following configuration methods.

Enable GSM/GPRS Antenna Fail/Restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → SMS REPORT → OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 12 us 1 #

SMS text message to all users simultaneously: 21 11 us 1 #

SMS delivery report: 55 11 us 1 #

Value: *us* - user phone number slot, range - [01... 10].
Example: *2512031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable GSM/GPRS Antenna Fail/Restore notification

EKB2

Menu path:
User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → SMS REPORT → OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:
User phone number: 25 12 us 0 #

SMS text message to all users simultaneously: 21 11 us 0 #

SMS delivery report: 55 11 us 0 #

Value: *us* - user phone number slot, range - [01... 10].
Example: *2512030#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

23. PARTITIONS

ESIM364 system comes equipped with a partitioning feature that can divide the alarm system into four independently controlled areas identified as Partition 1 through 4, which are all supervised by one alarm system unit. Partitioning can be used in installations where shared alarm system is more practical, such as a house and a garage or within a single multi-storey building. When partitioned, each system element, like zone, user phone number, keypad, user/master code, iButton key and wireless keyfob can be assigned to single or multiple partitions. The user will then be able to arm/disarm the system partition (-s) that the zones and arm/disarm method, except EKB2 keypad, are assigned to.

The following table reflects the values used for system element assignment to partitions by EKB2/EKB3/EKB3W keypad. A sum of values is used to assign the element to multiple partitions.

Partition	Value
Partition 1	1
Partition 2	2
Partition 3	4
Partition 4	8

Example1: The user wants to assign a certain iButton key to Partition 4 only. According to the table value 8 reflects Partition 4. He would then have to enter value 8.

Example2: The user wants to assign a certain user code to Partition 2 and 3. According to the table value 2 reflects Partition 2, while value 4 reflects Partition 3, therefore 2 + 4 = 6. He would then have to enter value 6.

Example3: The user wants to assign a certain zone to Partition 1, 3 and 4. According to the table value 1 reflects Partition 1, while values 4 and 8 reflect Partitions 3 and 4 respectively, therefore 1 + 4 + 8 = 13. He would then have to enter value 13.

23.1. Zone Partition

Zone partition determines which system partition (-s) the zone will operate in.

Set zone partition

EKB2

Menu path:
On-board zone: OK → iiii → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → PARTITION → OK → pv → OK
Wireless zone: OK → iiii → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → PARTITION → OK → pv → OK
Keypad zone: OK → iiii → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → PARTITION → OK → pv → OK
EPGM1 zone: OK → iiii → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → PARTITION → OK → pv → OK
Value: *iiii* – 4-digit installer code; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 57, zone number & partition value:
57 nn pv #
Value: *nn* – zone number, range – [01... 76]; *pv* – partition value (see **23. PARTITIONS**).
Example: *57032#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Wireless siren EWS1/EWS2/EWS3 siren will sound only if wireless zone of the siren is assigned to the same partition as the one that has been alarmed.

23.2. User Phone Number Partition

User phone number partition determines which system partition (-s) can be armed/disarmed from a certain user phone number by dialing system's phone number or sending an SMS text message.

Set user phone number partition

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → GSM USER 1... 10 → OK → PARTITION → pv → OK
Value: *iiii* – 4-digit installer code; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 59, user phone number slot & partition value:
59 us pv #
Value: *us* – user phone number slot, range – [01... 10]; *pv* – partition value (see **23. PARTITIONS**).
Example: *591013#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23.3. Keypad Partition and Keypad Partition Switch

Keypad partition determines which system partition the keypad will operate in. To identify which partition the keypad is operating in:

- EKB2 – Refer to partition name (by default – PART1) indicated in home screen view.
- EKB3W/EKB3 (2-partition mode) – Refer to the location of the illuminated indicator READY on the keypad. The indicator will be illuminated under section A or B, which represent Partition 1 and Partition 2 respectively.

EKB3 keypad can operate in the following modes:

- **2-partition mode** – This parameter determines whether EKB3 keypad can operate only in one of the first two system partitions allowing to arm/disarm them and switch the keypad partition using [1]... [2] keys. This mode is set up by default.

- **4-partition mode** – This parameter determines whether EKB3 keypad can operate in one of the four system partitions allowing to arm/disarm them, indicate arm/disarm status, zone state on [1]... [4] keys (see **32.1.2. EKB3 - LED Keypad**) and switch the keypad partition using [1]... [4] keys.

The keypad must be assigned to the same partition as the user/master code (see **23.4. User/Master Code Partition**) in order to arm/disarm the system by the keypad. For more details on system arming/disarming by the keypad, please refer to **12.3. EKB2 Keypad and User/Master Code**, **12.4. EKB3 Keypad and User/Master Code** and **12.5. EKB3W Keypad and User/Master Code..**

Set EKB3 partition mode as 2-partition or 4-partition

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

Set keypad partition

EKB2

Menu path:
EKB2 partition: OK → iiii → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → KEYPAD PARTITION → OK → [k] EKB2 → OK → PARTITION 1... 4 → OK → DISABLE | ENABLE → OK
EKB3 partition: OK → iiii → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → KEYPAD PARTITION → OK → [k] EKB3→ OK → PARTITION 1... 4 → OK
EKB3W partition: OK → iiii → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → EKB3W PARTITION → OK → EKB3W wless-id → OK → PARTITION 1... 2 → OK
Value: *iiii* – 4-digit installer code; *k* – keypad slot, range – [1... 4]; wless-id – 8-digit wireless device ID code.

EKB3/ EKB3W

Enter parameter 51, keypad slot & partition number:
EKB3 partition: 51 kk p #
EKB3W partition: 51 kw r #
Value: *kk* – EKB3 keypad slot, range – [01... 04]; *kw* – EB3W keypad slot, range – [05... 08]; *p* – EKB3 partition number, range – [1... 4]; *r* – EKB3W partition number, range – [1... 2].
Example: *51062#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: 4-partition mode must be enabled in order to assign EKB3 keypad to Partition 3 or Partition 4.

NOTE: EKB2 keypad can be assigned to multiple partitions, while EKB3 keypad can only be assigned only to single partition.

NOTE: EKB3W keypad assignment is restricted to Partition 1 and Partition 2.

NOTE: The slots for EKB3W keypads are automatically assigned to the bound keypad in the chronological order, hence the earliest bound keypad would acquire slot 5, while the latest bound keypad would acquire slot 8.

Keypad partition switch allows to quickly change the EKB3/EKB3W keypad partition. When the keypad partition is changed and when 1 minute after the last key-stroke/key-touch expires, the system will return to the preset keypad partition. Typically, this feature is used for viewing arm/ disarm status and alarms of a different partition or when arming/disarming a different system partition by EKB3/EKB3W keypad than the keypad is assigned to.

By default, keypad partition switch is disabled. To enable/disable this feature, please refer to the following configuration methods.

Enable keypad partition switch

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → PARTITION SWITCH → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 77 & parameter status value:
77 1#
Example: *771#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable keypad partition switch

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → PARTITION SWITCH → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 77 & parameter status value:
77 0 #
Example: *770#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Keypad partition switch can only be used when the system is partitioned.

23.4. User/Master Code Partition

User/master code partition determines which system partition (-s) can be armed/disarm using a certain user/master code. User/master code must be assigned to the same partition as the keypad (see **23.3. Keypad Partition and Keypad Partition Switch**) in order to arm/disarm the system by EKB2/EKB3/EKB3W keypad . For more details on system arming/disarming by the keypad, please refer to **12.3. EKB2 Keypad and User/Master Code**, **12.4. EKB3 Keypad and User/Master Code** and **12.5. EKB3W Keypad and User/Master Code**.

Set user/master code partition

EKB2

Master code: OK → mmmm → OK → CODES → OK → MASTER CODE → OK → PARTITION → OK → pv → OK
User code 2... 17: OK → mmmm → OK → CODES → OK → USER CODE (2-17) → OK → USER CODE 2... 17 → OK → PARTITION → OK → pv → OK
User code 18... 30: OK → mmmm → OK → CODES → OK → USER CODE (18-30) → OK → USER CODE 18... 30 → OK → PARTITION → OK → pv → OK
Value: *mmmm* – 4-digit master code; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Press [CODE], [5], 01/user code slot & enter master code:
Master code: [CODE] [5] 01 pv mmmm #
User code: [CODE] [5] us pv mmmm #
Value: *us* - user code slot, range - [02... 30]; *pv* – partition value (see **23. PARTITIONS**); *mmmm* - 4-digit master code.
Example: *CODE50481111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE for EKB3/EKB3W: User/master code partition management must be carried out using master code and without Configuration mode being activated.

23.5. iButton Key Partition

iButton key partition determines which system partition (-s) can be armed/disarmed using a certain key. iButton key must be assigned to the partition (-s) that the user desires to arm. For more details on system arming/disarming by iButton key, please refer to **12.5. iButton Key**.

Set iButton key partition

EKB2

Menu path:
OK → iiii → OK → IBUTTON KEYS → OK → IBUTTON → OK → IBUTTON 1... 16 → OK → PARTITION → OK → pv → OK
Value: *iiii* – 4-digit installer code; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 60, iButton key slot & partition value:
60 is pv #
Value: *is* – iButton key slot, range – [01... 16]; *pv* – partition value (see **23. PARTITIONS**).
Example: *600511#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23.6. EWK1/EWK2 Wireless Keyfob Partition

EWK1/EWK2 wireless keyfob partition determines which system partition can be armed/disarmed using a certain EWK1/EWK2 wireless keyfob. For more details on system arming/disarming by EWK1/EWK2 wireless keyfob, please refer to **12.6. EWK1/EWK2 Wireless Keyfob.**

Set EWK1/EWK2 partition

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: EWK1/EWK2 wireless keyfob can only be assigned to one partition.

24. TEMPERATURE SENSORS

The system may be equipped with up to 8 temperature sensors intended for temperature measurement in the surrounding areas. This feature allows to monitor the temperature of up to 8 different areas in real-time and receive a notification by SMS text message to User 1 phone number when the set temperature boundaries are exceeded. The temperature is measured at 0,5 degree centigrade (C) accuracy and automatically rounded to the higher value when 0,5 or above, e. g. temperature ranging from 23,5 through 24,4 will be treated as 24 C.

24.1. Adding, Removing and Replacing Temperature Sensors

To add a temperature sensor to the system, do the following:

a) Shutdown the system.

b) Wire up the temperature sensor to the 1-Wire interface terminals (see **2.3.5. Temperature Sensor and iButton Key Reader for temperature sensor wiring diagram**).

c) If more than one temperature sensor is required, wire another sensor in parallel to the previous one.

d) By default, the first added temperature sensor will be identified as primary and the second one – as secondary temperature sensor (see **24.2. Primary and Secondary Temperature Sensors**).

e) Add as many temperature sensors as necessary – wire up one after another in parallel – until the number of 8 sensors is reached.

f) Power up the system.

To view the real-time temperature values measured by each temperature sensor, please refer to the following configuration methods.

View real-time temperature values of individual temperature sensor

SMS

SMS text message content:
ssss_ITEMP:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_ITEMP:4*

EKB2

Menu path:
OK → uumm → OK → TEMP SENSORS INFO → OK → 1. tm.p C (PRIM) | (SEC)... 8. tm.p C
Value: *uumm* - 4-digit user/master code; *tm.p* – real-time temperature value.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View real-time temperature values of all temperature sensors

SMS

SMS text message content:
ssss_ITEMP:?
Value: *ssss* – 4-digit SMS password.
Example: *1111_ITEMP:?*

EKB2

Menu path:
OK → uumm → OK → TEMP SENSORS INFO → OK → 1. tm.p C (PRIM) | (SEC)... 8. tm.p C
Value: *uumm* - 4-digit user/master code; *tm.p* – real-time temperature value.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If a temperature sensor is faulty, it is recommended to remove it or replace it by a functional sensor.

Remove/replace individual temperature sensor

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: When multiple temperature sensors are connected, please touch and hold the sensor with your fingers and watch the temperature value change to identify the number of the temperature sensor slot.

24.2. Primary and Secondary Temperature Sensors

By default, the first added temperature sensor is automatically set as primary, while the second one is set as secondary temperature sensor. The real-time temperature values of the primary and secondary temperature sensors are included in the Info SMS text message (see **26. SYSTEM INFORMATION. INFO SMS**) as well as the temperature measured by the primary temperature sensor is indicated in the home screen view of EKB2 keypad.

To set a different temperature sensor as primary or secondary, please refer to the following configuration methods.

Set primary temperature sensor

SMS

SMS text message content:
ssss_TEMPI:PRIM:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_TEMPI:PRIM:4*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → PRIMARY TEMP SENS → OK → 1... 8 CONNECTED → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 89 & temperature sensor slot:
89 ts #
Value: *ts* – temperature sensor slot, range - [01... 08].
Example: *8903#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set secondary temperature sensor

SMS

SMS text message content:
ssss_TEMPI:SEC:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_TEMPI:SEC:3*

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → SECOND. TEMP SENS → OK → 1... 8 CONNECTED → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 90 & temperature sensor slot:
90 ts #
Value: *ts* – temperature sensor slot, range - [01... 08].
Example: *9005#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To view the slot number of primary and secondary temperature sensors, please refer to the following configuration methods.

View primary and secondary temperature sensor slot number

SMS

SMS text message content:
ssss_TEMPI:?
Value: *ssss* – 4-digit SMS password.
Example: *1111_TEMPI:?*

EKB2

Menu path:
Primary: OK → uumm → OK → TEMP SENSORS INFO → OK → 1... 8 tm.p C (PRIM)
Secondary: OK → uumm → OK → EMP SENSORS INFO → OK → 1... 8 tm.p C (SEC)
Value: uumm - 4-digit user/master code; tm.p – real-time temperature value.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View primary and secondary temperature sensor real-time temperature values

SMS

SMS text message content:
ssss_INFO
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO*

EKB2

Menu path:
Primary: OK → uumm → OK → TEMP SENSORS INFO → OK → 1... 8 tm.p C (PRIM)
Secondary: OK → uumm → OK → EMP SENSORS INFO → OK → 1... 8 tm.p C (SEC)
Value: uumm - 4-digit user/master code; tm.p – real-time temperature value.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Primary and secondary temperature sensors can be set by a single SMS text message, **Example:** *1111_TEMPI:PRIM:4,SEC:3*

24.3. Setting Up MIN and MAX Temperature Boundaries. Temperature Info SMS

The system supports an SMS text message identified as the Temperature Info SMS, which is automatically delivered to User 1 phone number if the preset minimum (MIN) or maximum (MAX) temperature boundary of any temperature sensor is exceeded by at least 1 C.

To set the MIN and MAX temperature boundaries for a certain temperature sensor, please refer to the configuration methods.

Set MIN and MAX temperature boundaries

SMS

SMS text message content:
ssss_TEMPts:MIN:mnn,MAX:mxx
Value: *ssss* – 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8]; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] C.
Example: *1111_TEMP2:MIN:-5,MAX:28*

EKB2

Menu path:
MIN: OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MIN → OK → mnn → OK
MAX: OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MAX → OK → mxx → OK
Value: *iiii* – 4-digit installer code; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] C.
Keys P1 or P2 are used to enter minus character, e.g. -20.

EKB3/ EKB3W

Enter parameter 19 & temperature Value:
19 ts mnn mxx #
Value: *ts* - temperature sensor slot, range – [1... 8]; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] C. 00 value stands for minus character, e. g. 0020 = -20
Example: *1906001530#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View MIN and MAX temperature boundaries

SMS

SMS text message content:
ssss_TEMPts
Value: *ssss* – 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8].
Example: *1111_TEMP4*

EKB2

Menu path:
MIN: OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MIN
MAX: OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MAX
Value: *iiii* – 4-digit installer code

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how *Send SMS text message to all users simultaneously* and *SMS delivery report* parameters affect the SMS text message transmission, please refer to **27. SYSTEM NOTIFICATIONS.**

NOTE: MIN and MAX boundaries can also be set separately by multiple SMS text messages, **Example:** *1111_TEMP1:MIN:6 and 1111_TEMP1:MAX:40*

24.4. Temperature Sensor Names

The temperature sensor name is included in the Temperature Info SMS when delivered to the User 1 phone number. This feature allows easier identification of the temperature sensor and normally it is used when monitoring temperature changes in different areas.

Set temperature sensor name

SMS **SMS text message content:**
ssss_TEMPts:NAME:temp-sens-name
Value: *ssss* - 4-digit SMS password; *ts* - temperature sensor slot, range - [1... 8]; *temp-sens-name* - 4 to 24 characters temperature sensor name.
Example: *1111_TEMP3:NAME:Warehouse*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View temperature sensor name

SMS **SMS text message content:**
ssss_TEMPts
Value: *ssss* - 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8].
Example: *1111_TEMP3*

EKB2 **Menu path:**
OK → iiii → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → NAME
Value: *iiii* – 4-digit installer code.

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete temperature sensor name

SMS **SMS text message content:**
ssss_TEMPts:NAME:
Value: *ssss* - 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8].
Example: *1111_TEMP2:NAME:*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

25. REMOTE LISTENING AND 2-WAY VOICE COMMUNICATION

ESIM364 comes equipped with a microphone that allows the user to listen on his mobile phone to what is happening in the secured area. By installing one of the audio modules EA1 or EA2, the user will be able to have a 2-way voice communication (see **32.3.2. EA1 - Audio Output Module** and **32.3.3. EA2 - Audio Output Module with Amplifier**). Remote listening and 2-way voice communication can operate under the following conditions:

- The system makes a phone call via GSM to a preset user phone number in case of alarm and the user answers the call.
- The user initiates remote listening by sending the SMS text message, the system makes a phone call via GSM to the user phone number that the SMS text message was sent from and the user answers the call.

Initiate remote listening

SMS

SMS text message content:
ssss_MIC
Value: *ssss* - 4-digit SMS password.
Example: *1111_MIC*

Set microphone gain

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → GSM AUDIO → OK → MICROPHONE GAIN → OK → mg → OK
Value: *iiii* – 4-digit installer code; *mg* – microphone gain, range – [0... 15].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set speaker level

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → GSM AUDIO → OK → SPEAKER LEVEL → OK → sl → OK
Value: *iiii* – 4-digit installer code; *sl* – speaker level, range – [0... 85].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Phone calls to the preset user phone number in case of alarm are disabled by force when MS mode is enabled (see **30. MONITORING STATION).**

26. SYSTEM INFORMATION. INFO SMS

The system supports an informational SMS text message identified as the Info SMS, which can be delivered upon request. Once requested, the system will reply with Info SMS that provides the following:

- System date & time.
- System status: partition armed (ON)/disarmed (OFF).
- GSM signal strength.
- Mains power supply status.
- Temperature of the area surrounding primary and secondary temperature sensors (if any).
- State of zones (OK/alarm).
- Name and status (ON/OFF) of PGM outputs.

Request for system information

SMS

SMS text message content:
ssss_INFO
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

26.1. Periodic Info SMS

By default, the system sends Info SMS to User 1 phone number periodically once a day at 11:00 (frequency – 1 day; time – 11). The minimum period is every 1 hour (frequency – 0 days; time – 1). Typically, this feature is used to verify the power supply and online status of the system.

To set a different frequency and time or disable periodic Info SMS, please refer to the following configuration methods.

Set periodic Info SMS frequency and time

SMS

SMS text message content:
ssss_INFO:fff:it
Value: *ssss* – 4-digit SMS password; *fff* – frequency, range – [00... 99] days; *it* – time, range – [01... 23].
Example: *1111_INFO:3.15*

EKB2

Menu path:
Frequency: OK → iiii → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → FREQUENCY (DAYS) → fff → OK
Time: OK → iiii → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → TIME → it → OK
Value: *iiii* – 4-digit installer code; *fff* – frequency, range – [00... 125] days; *it* – time, range – [01... 23].

EKB3/ EKB3W

Enter parameter 11, time & frequency:
11it fff #
Value: *it* – time, range – [01... 23]; *fff* – frequency, range – [00... 125] days.
Example: *110412#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable periodic Info SMS

SMS

SMS text message content:
ssss_INFO:00:00
Example: *1111_INFO:00.00*

EKB2

Menu path:
Frequency: OK → iiii → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → FREQUENCY (DAYS) → 0 → OK
Time: OK → iiii → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → TIME → 0 → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 11, time & frequency:
11 00 00 #
Example: *110000#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Unlike Info SMS upon request, periodic Info SMS text message does not included zone states, PGM output names and status.

27. SYSTEM NOTIFICATIONS

By default in case of a certain event, the system attempts to send an SMS text message to the first preset user phone number only. If the user phone number is unavailable and the system fails to receive the SMS delivery report during 20 seconds, it will attempt to send the SMS text message to the next preset user phone number, assigned to the same partition as the previous one. The user phone number may be unavailable due to the following reasons:

- mobile phone was switched off.
- was out of GSM signal coverage.

The system will continue sending the SMS text message to the next preset user phone numbers in the priority order until one is available. The system sends the SMS text message only once and will not return to the first user phone number if the last one was unavailable.

To change the SMS text message delivery algorithm, user can enable/disable the following parameters for certain events:

- **Send SMS text message to all users simultaneously** - This parameter determines whether to ignore the SMS delivery report or not. Once enabled, the system will attempt to send the SMS text message to every preset user phone number that is enabled to receive a certain event from the system by SMS text message. In addition, this parameter overrides the SMS delivery report parameter regardless of the SMS delivery report parameter's status (enabled/disabled).
- **SMS delivery report** - This parameter determines whether to request for SMS delivery report or not. Once disabled, the system will not verify the status of the SMS text message delivery and will attempt to deliver the SMS text message only to the first preset user phone number regardless if the next preset user phone number (-s) is enabled to receive a certain event by SMS text message or not.
- **Send SMS text message to all users simultaneously** - By default, the system sends SMS text message to the first available user in case of alarm. If the system did not receive the SMS delivery report during 20 seconds, it will attempt to send the SMS text message to the next preset user phone number. To ignore the SMS delivery report and allow/disallow the system to send the SMS text message to every preset user phone number, please refer to the following configuration methods.

When using Dual-SIM feature, the Secondary SIM card is involved in the communication process. For more details, please refer to **31. DUAL SIM MANAGEMENT.**

The following table provides the description of system notifications by SMS text message sent to the user phone number.

Seq. No.	**Event**	**Description**
1	System armed	SMS text message sent to the user regarding armed system.
2	System disarmed	SMS text message sent to the user about disarmed system.
3	General alarm	SMS text message sent to the user in case of system alarm occurrence.
4	Mains power loss/ restore	SMS text message sent to the user in case the mains power supply is lost or restored
5	Battery failed	SMS text message sent to the user in case the backup battery resistance is 2Ω or higher (battery requires replacement).
6	Battery dead or missing	SMS text message sent to the user in case the backup battery is not present or the battery voltage runs below 5V.
7	Low battery	SMS text message sent to the user in case the backup battery voltage is 10.5V or lower.
8	Siren fail/restore	SMS text message sent to the user in case the siren is disconnected/broken or connected/fixed.
9	Date/time not set	SMS text message sent to the user in case system date & time is not set.
10	GSM connection failed	SMS text message sent to the user in case the GSM connection is lost.
11	GSM/GPRS antenna fail/restore	SMS text message sent to the user in case the GSM/GPRS antenna is disconnected/broken or connected/broken.
12	Tamper alarm	SMS text message sent to the user in case of tamper violation. Indicated as *Tamper x*.
13	Keypad failed	SMS text message sent to the user in case the keypad is disconnected/broken.
14	Temperature info	SMS text message sent to the user in case of temperature deviation by the set values.
15	System started	SMS text message sent to the user on system startup.
16	Periodical info	Info SMS text message sent to the user periodically by the set values.
17	Wireless signal loss	SMS text message sent to the user in case the wireless signal is lost. Indicated as *No wireless signal from wless-dev wless-id Tamper x*
18	Unable to arm	SMS text message sent to the user in case the system denies arming due to existing violated zone (-s)/tamper (-s).

To enable/disable a certain system notification, please refer to the following configuration methods.

Disable system notification

EKB2

Menu path:

System armed:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → SMS REPORT → OK → DISABLE → OK

System disarmed:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → SMS REPORT → OK → DISABLE → OK

General alarm:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM EV → OK → SMS REPORT → OK → DISABLE → OK

Mains power loss/restore:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R EV → OK → SMS REPORT → OK → DISABLE → OK

Battery failed:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → SMS REPORT → OK → DISABLE → OK

Battery dead or missing:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → SMS REPORT → OK → DISABLE → OK

Low battery:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY EVENT → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY EVENT → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY EVENT → OK → SMS REPORT → OK → DISABLE → OK

Siren fail/restore:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → SMS REPORT → OK → DISABLE → OK

Date/time not set:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → DATE/TIME NOT SET → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → DATE/TIME NOT SET → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → DATE/TIME NOT SET → OK → SMS REPORT → OK → DISABLE → OK

GSM connection failed:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → SMS REPORT → OK → DISABLE → OK

GSM/GPRS antenna fail/restore:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → SMS REPORT → OK → DISABLE → OK

Tamper alarm:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → SMS REPORT → OK → DISABLE → OK

Keypad failed:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → KEYPAD FAILED→ OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → KEYPAD FAILED → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → KEYPAD FAILED → OK → SMS REPORT → OK → DISABLE → OK

Temperature info:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → TEMP INFO EVENT→ OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → TEMP INFO EVENT → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → TEMP INFO EVENT → OK → SMS REPORT → OK → DISABLE → OK

System started:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → SYSTEM STARTED EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → SYSTEM STARTED EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → SYSTEM STARTED EV → OK → SMS REPORT → OK → DISABLE → OK

Periodical info:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → PERIOD INFO SMS EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → PERIOD INFO SMS EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → PERIOD INFO SMS EV → OK → SMS REPORT → OK → DISABLE → OK

Wireless signal loss:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → SMS REPORT → OK → DISABLE → OK

Unable to arm:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → FAIL TO ARM SMS → OK → GSM USER 1... 10 → OK → DISABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → FAIL TO ARM SMS → OK → SMS TO ALL → OK → DISABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → FAIL TO ARM SMS → OK → SMS REPORT → OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:

System armed event

User phone number: 25 01 up 0 #

SMS text message to all users simultaneously: 21 01 up 0 #

SMS delivery report: 55 01 up 0 #

System disarmed event

User phone number: 25 02 up 0 #

SMS text message to all users simultaneously: 21 02 up 0 #

SMS delivery report: 55 02 up 0 #

General alarm

User phone number: 25 03 up 0 #

SMS text message to all users simultaneously: 21 03 up 0 #

SMS delivery report: 55 03 up 0 #

Main power loss/restore

User phone number: 25 04 up 0 #

SMS text message to all users simultaneously: 21 04 up 0 #

SMS delivery report: 55 04 up 0 #

Battery failed

User phone number: 25 05 up 0 #

SMS text message to all users simultaneously: 21 05 up 0 #

SMS delivery report: 55 05 up 0 #

Battery dead or missing

User phone number: 25 06 up 0 #

SMS text message to all users simultaneously: 21 06 up 0 #

SMS delivery report: 55 06 up 0 #

Low battery

User phone number: 25 07 up 0 #

SMS text message to all users simultaneously: 21 07 up 0 #

SMS delivery report: 55 07 up 0 #

Siren fail/restore
User phone number: 25 08 up 0 #
SMS text message to all users simultaneously: 21 08 up 0 #
SMS delivery report: 55 08 up 0 #

Date/time not set
User phone number: 25 10 up 0 #
SMS text message to all users simultaneously: 21 10 up 0 #
SMS delivery report: 55 10 up 0 #

GSM connection failed
User phone number: 25 11 up 0 #
SMS text message to all users simultaneously: 21 11 up 0 #
SMS delivery report: 55 11 up 0 #

GSM/GPRS antenna fail/restore
User phone number: 25 12 up 0 #
SMS text message to all users simultaneously: 21 12 up 0 #
SMS delivery report: 55 12 up 0 #

Tamper alarm
User phone number: 25 13 up 0 #
SMS text message to all users simultaneously: 21 13 up 0 #
SMS delivery report: 55 13 us 0 #

Keypad failed
User phone number: 25 14 up 0 #
SMS text message to all users simultaneously: 21 14 up 0 #
SMS delivery report: 55 14 up 0 #

Temperature info
User phone number: 25 15 up 0 #
SMS text message to all users simultaneously: 21 15 up 0 #
SMS delivery report: 55 15 up 0 #

System started
User phone number: 25 16 up 0 #
SMS text message to all users simultaneously: 21 16 up 0 #
SMS delivery report: 55 16 up 0 #

Periodical info
User phone number: 25 17 up 0 #
SMS text message to all users simultaneously: 21 17 up 0 #
SMS delivery report: 55 17 up 0 #

Wireless signal loss
User phone number: 25 18 up 0 #
SMS text message to all users simultaneously: 21 18 up 0 #
SMS delivery report: 55 18 up 0 #

Unable to arm
User phone number: 25 19 up 0 #
SMS text message to all users simultaneously: 21 19 up 0 #
SMS delivery report: 55 19 up 0 #

Value: *up* - user phone number slot, range - [01... 10].
Example: *2514020*#

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable system notification

EKB2

Menu path:

System armed:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS ARMED EVENT → OK → SMS REPORT → OK → ENABLE → OK

System disarmed:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SYS DISARMED EVENT → OK → SMS REPORT → OK → ENABLE→ OK

General alarm:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → GENERAL ALARM EV → OK → SMS REPORT → OK → ENABLE → OK

Mains power loss/restore:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R EV → OK → SMS REPORT → OK → ENABLE→ OK

Battery failed:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY FAILED → OK → SMS REPORT → OK → ENABLE → OK

Battery dead or missing:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → SMS REPORT → OK → ENABLE → OK

Low battery:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY EVENT → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → LOW BATTERY EVENT → OK → SMS REPORT → OK → ENABLE → OK

Siren fail/restore:

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → SMS REPORT → OK → ENABLE → OK

User phone number: OK → iiii → OK → SMS MESSAGES 1 → OK → DATE/TIME NOT SET → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 1 → OK → DATE/TIME NOT SET → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 1 → OK → DATE/TIME NOT SET → OK → SMS REPORT → OK → ENABLE → OK

GSM connection failed:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → SMS TO ALL → OK → DENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → SMS REPORT → OK → ENABLE → OK

GSM/GPRS antenna fail/restore:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → SMS REPORT → OK → ENABLE → OK

Tamper alarm:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → SMS REPORT → OK → ENABLE → OK

Keypad failed:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → KEYPAD FAILED→ OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → KEYPAD FAILED → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → KEYPAD FAILED → OK → SMS REPORT → OK → ENABLE → OK

Temperature info:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → TEMP INFO EVENT→ OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → TEMP INFO EVENT → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → TEMP INFO EVENT → OK → SMS REPORT → OK → ENABLE → OK

System started:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → SYSTEM STARTED EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → SYSTEM STARTED EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → SYSTEM STARTED EV → OK → SMS REPORT → OK → ENABLE → OK

Periodical info:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → PERIOD INFO SMS EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → PERIOD INFO SMS EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → PERIOD INFO SMS EV → OK → SMS REPORT → OK → ENABLE → OK

Wireless signal loss:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → SMS REPORT → OK → ENABLE → OK

Unable to arm:

User phone number: OK → iiii → OK → SMS MESSAGES 2 → OK → FAIL TO ARM SMS → OK → GSM USER 1... 10 → OK → ENABLE → OK

SMS text message to all users simultaneously: OK → iiii → OK → SMS MESSAGES 2 → OK → FAIL TO ARM SMS → OK → SMS TO ALL → OK → ENABLE → OK

SMS delivery report: OK → iiii → OK → SMS MESSAGES 2 → OK → FAIL TO ARM SMS → OK → SMS REPORT → OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 25/21/55, event number, user phone number slot & parameter status value:

System armed event

User phone number: 25 01 up 1 #

SMS text message to all users simultaneously: 21 01 up 1 #

SMS delivery report: 55 01 up 1 #

System disarmed event

User phone number: 25 02 up 1 #

SMS text message to all users simultaneously: 21 02 up 1 #

SMS delivery report: 55 02 up 1 #

General alarm

User phone number: 25 03 up 1 #

SMS text message to all users simultaneously: 21 03 up 1 #

SMS delivery report: 55 03 up 1 #

Main power loss/restore

User phone number: 25 04 up 1 #

SMS text message to all users simultaneously: 21 04 up 1 #

SMS delivery report: 55 04 up 1 #

Battery failed

User phone number: 25 05 up 1 #

SMS text message to all users simultaneously: 21 05 up 1 #

SMS delivery report: 55 05 up 1 #

Battery dead or missing

User phone number: 25 06 up 1 #

SMS text message to all users simultaneously: 21 06 up 1 #

SMS delivery report:55 06 up 1 #

Low battery

User phone number: 25 07 up 1 #

SMS text message to all users simultaneously: 21 07 up 1 #

SMS delivery report:55 07 up 1 #

Siren fail/restore

User phone number: 25 08 up 1 #

SMS text message to all users simultaneously: 21 08 up 1 #

SMS delivery report: 55 08 up 1 #

Date/time not set
User phone number: 25 10 up 1 #
SMS text message to all users simultaneously: 21 10 up 1 #
SMS delivery report: 55 10 up 1 #

GSM connection failed
User phone number: 25 11 up 1 #
SMS text message to all users simultaneously: 21 11 up 1 #
SMS delivery report: 55 11 up 1 #

GSM/GPRS antenna fail/restore
User phone number: 25 12 up 1 #
SMS text message to all users simultaneously: 21 12 up 1 #
SMS delivery report: 55 12 up 1 #

Tamper alarm
User phone number: 25 13 up 1 #
SMS text message to all users simultaneously: 21 13 up 1 #
SMS delivery report: 55 13 up 1 #

Keypad failed
User phone number: 25 14 up 1 #
SMS text message to all users simultaneously: 21 14 up 1 #
SMS delivery report: 55 14 up 1 #

Temperature info
User phone number: 25 15 up 1 #
SMS text message to all users simultaneously: 21 15 up 1 #
SMS delivery report: 55 15 up 1 #

System started
User phone number: 25 16 up 1 #
SMS text message to all users simultaneously: 21 16 up 1 #
SMS delivery report: 55 16 up 1 #

Periodical info
User phone number: 25 17 up 1 #
SMS text message to all users simultaneously: 21 17 up 1 #
SMS delivery report: 55 17 up 1 #

Wireless signal loss
User phone number: 25 18 up 1 #
SMS text message to all users simultaneously: 21 18 up 1 #
SMS delivery report: 55 18 up 1 #

Unable to arm
User phone number: 25 19 up 1 #
SMS text message to all users simultaneously: 21 19 up 1 #
SMS delivery report: 55 19 up 1 #

Value: *up* - user phone number slot, range - [01... 10].
Example: *2517041#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

27.1. SMSC (Short Message Service Center) Phone Number

An SMS center (SMSC) is a GSM network element, which routes SMS text messages to the destination user and stores the SMS text message if the recipient is unavailable. Typically, the phone number of the SMS center is already stored in the SIM card provided by the GSM operator. If the user fails to receive replies from the system, the SMS center phone number, provided by the GSM operator, must be set manually.

Set SMSC phone number

SMS

SMS text message content:
ssss_SMS_+ttteeellnnuumm

Value: *ssss* – 4-digit SMS password; *ttteeellnnuumm* – up to 15 digits SMSC phone number.
Example: *1111_SMS_+4417031111111*

ATTENTION: Before setting the SMSC phone number, please check the credit balance of the system's SIM card. The system will fail to reply if the credit balance is insufficient.

28. EVENT AND ALARM LOG

The event log allows to chronologically register up to 500 timestamped records regarding the following system events:

- System start.
- System arming/disarming.
- Zone violated/restored.
- Tamper violated/restored.
- Zone bypassing.
- Wireless device management.
- Temperature deviation by MIN and MAX boundaries.
- System faults.

The event log is of LIFO (last in, first out) type that allows the system to automatically replace the oldest records with the the latest ones.

View event log

EKB2

Menu path:
OK → mmmm → OK → VIEW EVENT LOG → OK
Value: *mmmm* - 4-digit master code.

To export the event log to .log file or clear it, please refer to the following configuration method.

Export/clear event log

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, event log is enabled. To disable/enable this feature, please refer to the following configuration methods.

Disable event log

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → EVENT LOG → OK → DISABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 36 and parameter status value:
36 0 #
Example: *360#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable event log

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETTINGS → OK → EVENT LOG → OK → ENABLE → OK
Value: *iiii* - 4-digit installer code.

EKB3/ EKB3W

Enter parameter 36 and parameter status value:
36 1 #
Example: *361#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The alarm log provides a list of last 16 alarm events generated after last arming period. The alarm log can be viewed via EKB2 and includes only the alarms of the partition that the user/master code is assigned to. Each alarm record includes alarm type, partition number and zone number. When highlighted, the date and time of the alarm occurrence can be viewed at the bottom of EKB2 screen. In case of alarm, 🔊 icon will appear in home screen view of EKB2. The alarm log auto-clears when the next system arming follows or after viewing it via the keypad.

View alarm log

EKB2

Menu path:
OK → uumm → OK → ALARM LOG → OK
Value: *uumm* - 4-digit user/master code.

29. INDICATION OF SYSTEM FAULTS

The system comes equipped with self-diagnostic feature allowing to indicate the presence of any system fault by the keypad as well as by SMS text message notification to the preset user phone number. By default the indication for all system faults is indicated on the keypad. To disable/enable the indication of a certain system fault, please refer to the following configuration method.

Disable/enable individual system fault indication on keypad

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: After enabling/disabling a certain system fault indication, it is necessary to restart the system locally by powering down and powering up the system the system or remotely (see **35. REMOTE SYSTEM RESTART**).

EN50131-1 **GRADE 3**

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following feature:

- System arming is blocked if any system fault exists. The user wil not be able to arm the system until all existing system faults are solved.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **36. EN 50131-1 GRADE 3.**

EKB2

🔧! icon displayed in home screen view indicates presence of system faults. In order to view the currently present system faults, please enter a valid user/master code to access menu section **FAULTS**. The description on each system fault is provided in the table below.

Menu path:

OK → uumm → OK → FAULTS → OK

Value: *uumm* – 4-digit user/master code.

Name	Description
MAIN POWER LOSS	Mains power supply is lost
LOW BATTERY	Low backup battery power - backup battery voltage is 10.5V or lower
BATTERY DEAD/MISS	Backup battery is not present or the battery voltage runs below 5V
BATTERY FAILED	Backup battery requires replacement - backup battery resistance is 2Ω or higher
SIREN FAILED	Siren is disconnected/broken
VIOLATED TAMPER	One or more tampers are violated
DATE/TIME NOT SET	Date/time not set
GSM CONNECT FAILED	GSM connection is lost
GSM/GPRS ANTENNA FAILED	GSM/GPRS antenna is disconnected/broken
WLESS ANTENNA FAIL	Wireless antenna is disconnected/broken
KEYPAD LOST	Keypad is disconnected/broken

Yellow LED **SYSTEM** indicates system faults. **SYSTEM** LED indications are mentioned in the table below.

SYSTEM LED	Description
Illuminated continously	One or more tampers are violated; other system faults (see below)
Flashing	One or more high-numbered zones are violated

In order to find out more on the particular system fault, please enter command A provided below. After this procedure the system will activate red zone LEDs for 15 seconds. The description on each LED indication is mentioned in the table below.

Zone LED	Description
1	Mains power supply is lost
2	Low backup battery power - backup battery voltage is 10.5V or lower
3	Backup battery is not present or the battery voltage runs below 5V
4	Backup battery requires replacement - backup battery resistance is 2Ω or higher
5	Siren is disconnected/broken
7	One or more tampers are violated
8	Date/time not set
9	One or more high-numbered zones (Z13-Z76) are violated
10	GSM connection is lost
11	GSM/GPRS antenna is disconnected/broken
12	Wireless antenna is disconnected/broken

In order to find out which particular high-numbered zone is violated please , enter command B.

In order to find out which particular tamper is violated please , enter command C.

A. System fault indication - enter command:
[CODE#]

B. Violated high-numbered zone indication – enter command:
[CODE1]

C. Violated tamper indication – enter command:
[CODE2]

The number of violated high-numbered zone or tamper can be calculated using the table below according to the formula: number from zone LED section B + number from zone LED section A.

Example: LED #3 from section A is flashing and LED #8 from section B is illuminated continuously. According to the table below LED #8 is equal to number 18, therefore 18 + 3 = 21.

Result: Violated high-numbered zone or tamper number is 21.

Zone LED section - A (flashing)	Zone LED section - B (illuminated continously)
Zone LED 1 = 1	Zone LED 7 = 12
Zone LED 2 = 2	Zone LED 8 = 18
Zone LED 3 = 3	Zone LED 9 = 24
Zone LED 4 = 4	Zone LED 10 = 30
Zone LED 5 = 5	Zone LED 11 = 36
Zone LED 6 = 6	Zone LED 12 = 42

30. MONITORING STATION

The system can be configured to report events to the monitoring station by transmitting data messages to the monitoring station. The system connects to the monitoring station when the MS (Monitoring Station) mode is enabled.

Enable MS mode

SMS

SMS text message content:
ssss_SCNSET:ON
Value: *ssss* – 4-digit SMS password.
Example: *1111_SCNSET:ON*

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → MS MODE → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 23 & parameter status value:
23 1 #
Example: *231#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable MS mode

SMS

SMS text message content:
ssss_SCNSET:OFF
Value: *ssss* – 4-digit SMS password.
Example: *1111_SCNSET:OFF*

EKB2

Menu path:
OK →iiii → OK → MS SETTINGS → OK → MS MODE → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 23 & parameter status value:
23 0 #
Example: *230#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Account is a 4-digit number (By default – 9999) required to identify the alarm system unit by the monitoring station.

Set account

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → ACCOUNT → OK → cccc → OK
Value: *iiii* – 4-digit installer code; *cccc* – 4-digit account number.

EKB3/ EKB3W

Enter parameter 27 & account number:
27 cccc #
Value: *cccc* – 4-digit account number.
Example: *278853#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: The system will NOT send any data to the monitoring station while remote configuration, remote firmware update or remote listening/2-way voice communication is in progress. However, during the remote configuration session, firmware update process or remote listening/2-way voice communication process, the data messages will be queued up and transmitted to the monitoring station after the remote configuration session, firmware update or remote listening/2-way voice communication process is over.

ATTENTION: Phone calls to the preset user phone number via GSM in case of alarm are disabled by force when MS mode is enabled.

30.1. Data Messages - Events

The configuration of data messages is based on Ademco Contact ID protocol. The data messages can either be transmitted to the monitoring station alone or with duplication by SMS text message to preset user phone number. For more details on system notifications by SMS text message, please refer to **27. SYSTEM NOTIFICATIONS**.

Seq. No.	Contact ID® Code	Event	Description
1	1110	Fire alarm	Transmitted in case a zone of Fire type is violated.
2	3110	Fire restore	Transmitted in case a zone of Fire type is restored.
3	1121	Disarmed by user (Duress code)	Transmitted in case the system is disarmed by Duress code.
4	1130	Burglary alarm	Transmitted in case a zone of Delay (if not disarmed before entry delay countdown is completed), Interior Follower or Instant type is violated.
5	3130	Burglary restore	Transmitted in case a zone of Delay (if not disarmed before entry delay countdown is completed), Interior Follower or Instant type is restored.
6	1133	24-Hour zone alarm	Transmitted in case of zone of 24-Hour type is violated.
7	3133	24-Hour zone restore	Transmitted in case of zone of 24-Hour type is restored.
8	1144	Tamper alarm	Transmitted in case the tamper is violated.
9	3144	Tamper restore	Transmitted in case the tamper is restored.
10	1146	Panic/Silent zone alarm	Transmitted in case of zone of Panic/Silent type is violated.
11	3146	Panic/Silent zone restore	Transmitted in case of zone of Panic/Silent type is restored.
12	1158	Temperature risen	Transmitted in case of the temperature has increased above the MAX set value.
13	1159	Temperature fallen	Transmitted in case of temperature has decreased below the MIN set value.
14	1301	Mains power loss	Transmitted in case the main power supply is lost.
15	3301	Mains power restore	Transmitted in case the main power supply is restored.
16	1302	Low battery	Transmitted in case the backup battery voltage is 10.5V or lower / the wireless sensor battery level runs below 5%.
17	1308	System shutdown	When the system is running on backup battery power, it transmits the data message before the backup battery power is fully depleted.
18	1309	Battery failed	Transmitted in case the backup battery resistance is 2Ω or higher.
19	1311	Battery dead or missing	Transmitted in case the backup battery is not present or the battery voltage runs below 5V.
20	3311	Battery connection restore	Transmitted in case the backup battery connecton is fixed.
21	1321	Siren fail	Transmitted in case the siren is disconnected/broken.
22	3321	Siren restore	Transmitted in case the siren is connected/fixed.
23	1330	Keypad fail	Transmitted in case the keypad is disconnected/broken.
24	3330	Keypad restore	Transmitted in case the keypad is connected/fixed
25	1354	GPRS connection loss	Transmitted in case the GPRS connection is lost.
26	1358	GSM connection failed	Transmitted in case the GSM connection is lost.
27	1359	GSM/GPRS antenna fail	Transmitted in case the GSM/GPRS antenna is disconnected/broken
28	3359	GSM/GPRS antenna restore	Transmitted in case the GSM/GPRS antenna is connected/fixed.
29	1381	Wireless signal loss	Transmitted in case the connection with any wireless device is lost.
30	3381	Wireless signal restore	Transmitted in case the connection with any wireless device is restored.
31	1401	Disarmed by user	Transmitted in case the system is disarmed.
32	3401	Armed by user	Transmitted in case the system is armed.
33	1456	Disarmed in Stay mode	Transmitted in case the system is disarmed in Stay mode.
34	3456	Armed in Stay mode	Transmitted in case the system is armed in Stay mode.
35	1463	Disarmed by user (SGS code)	Transmitted in case the system is disarmed by SGS code.
36	3463	Armed by user (SGS code)	Transmitted in case the system is armed by SGS code.
37	1570	Zone bypassed	Transmitted in case a violated zone is bypassed.
38	3570	Bypassed zone activated	Transmitted in case a bypassed zone is activated.
39	1602	Test event/Kronos ping	Transmitted for system online status verification purposes.
40	3626	Date/time not set	Transmitted in case system date & time is not set.
41	1900	System started	Transmitted on system startup.

The following table refers to user codes included in arm/disarm data messages.

Type	Code
User Phone Number 1	0
User Phone Number 2	1
User Phone Number 3	2
User Phone Number 4	3
User Phone Number 5	4
User Phone Number 6	5
User Phone Number 7	6
User Phone Number 8	7
User Phone Number 9	8
User Phone Number 10	9
iButton 1	10
iButton 2	11
iButton 3	12
iButton 4	13
iButton 5	14
iButton 6	15
iButton 7	16
iButton 8	17
iButton 9	18
iButton 10	19
iButton 11	20
iButton 12	21
iButton 13	22
iButton 14	23
iButton 15	24
iButton 16	25
Master Code	26
User Code 2	27
User Code 3	28
User Code 4	29
User Code 5	30
User Code 6	31
User Code 7	32
User Code 8	33
User Code 9	34
User Code 10	35
User Code 11	36
User Code 12	37
User Code 13	38
User Code 14	39
User Code 15	40
User Code 16	41
User Code 17	42
User Code 18	43
User Code 19	44
User Code 20	45
User Code 21	46
User Code 22	47
User Code 23	48
User Code 24	49
User Code 25	50
User Code 26	51
User Code 27	52
User Code 28	53
User Code 29	54
User Code 30	55
Remote Code (EGR100)	56
KeyFob 1	133
KeyFob 2	134
KeyFob 3	135

KeyFob 4	136
KeyFob 5	137
Arm/Disarm by Zone	213

Disable data message

EKB2

Menu path:

Burglary alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → BURGLR ALM/REST EV → OK → DISABLE → OK

Mains power loss/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → MAIN POWER L/R EV → OK → DISABLE → OK

Armed/disarmed by user: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → ARM/DISARM EVENT → OK → DISABLE → OK

Battery failed: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → BATTERY FAILED → OK → DISABLE → OK

Battery dead or missing/battery connection restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → DISABLE → OK

Test event: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → TEST EVENT → OK → DISABLE → OK

Tamper alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → TAMPER ALM/REST EV → OK → DISABLE → OK

Panic/Silent zone alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → PA/SIL ALM/REST EV → OK → DISABLE → OK

System started: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → SYSTEM STARTED EV → OK → DISABLE → OK

Fire alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → FIRE ALM/REST EV → OK → DISABLE → OK

24-Hour zone alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → 24H ALM/REST EVENT→ OK → DISABLE → OK

Low battery: OK → iiii → OK → MS SETTINGS → OK →DATA MESSAGES 1 → OK → LOW BATTERY EVENT → OK → DISABLE → OK

Temperature risen: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → TEMP HIGH EVENT → OK → DISABLE → OK

Temperature fallen: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → TEMP LOW EVENT → OK → DISABLE → OK

Wireless signal loss/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → WLESS SIGN L/R EV → OK → DISABLE → OK

Disarmed by user (Duress code): OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → DISARM DURESS EV → OK → DISABLE → OK

Armed/disarmed by user (SGS code): OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → ARM/DARM SGS EVENT → OK → DISABLE → OK

Armed/disarmed in Stay mode: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → ARM/DARM STAY EV → OK → DISABLE → OK

Siren fail/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → SIREN FAIL/REST EV → OK → DISABLE → OK

Date/time not set: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → DATE/TIME NOT SET → OK → DISABLE → OK

GSM connection failed: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → GSM CONNECT FAILED → OK → DISABLE → OK

GSM/GPRS antenna fail/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → DISABLE → OK

System shutdown: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → SYSTEM SHUTDOWN EV → OK → DISABLE → OK

Keypad fail/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → KEYPAD FAIL/REST → OK → DISABLE → OK

GPRS connection failed: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → GPRS CONNECT FAIL → OK → DISABLE → OK

Zone bypassed/activated: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → ZONE BYPASS→ OK → DISABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/
EKB3W

Enter parameter 24, event number & parameter status value:
24 01 0 # – Burglary alarm/restore
24 02 0 # – Mains power loss/restore
24 03 0 # – Armed/disarmed by user
24 04 0 # – Test event
24 05 0 # – Battery failed
24 06 0 # –Battery dead or missing/battery connection restore
24 07 0 # – Tamper alarm/restore
24 08 0 # – Panic/Silent zone alarm/restore
24 09 0 # – Kronos ping
24 10 0 # – System started
24 13 0 # – 24-Hour zone alarm/restore
24 14 0 # – Fire zone alarm/restore
24 15 0 # – Low battery
24 16 0 # –Temperature risen
24 17 0 # – Temperature fallen
24 18 0 # – Wireless signal loss/restore
24 19 0 # – Disarmed by user (Duress code)
24 20 0 # – Armed/disarmed by user (SGS code)
24 21 0 # – Armed/disarmed in Stay mode
24 22 0 # – Siren fail/restore
24 24 0 # –Date/time not set
24 25 0 # – GSM connection failed
24 26 0 # – GSM/GPRS antenna fail/restore
24 27 0 # – System shutdown
24 28 0 # – Keypad fail/restore
24 29 0 # – GPRS connection failed
24 30 0 # – Zone bypassed/activated
Example: *24080#*

Config
Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable data message

EKB2

Menu path:

Burglary alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → BURGLR ALM/REST EV → OK → ENABLE → OK

Mains power loss/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → MAIN POWER L/R EV → OK →ENABLE → OK

Armed/disarmed by user: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → ARM/DISARM EVENT → OK → ENABLE → OK

Battery failed: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → BATTERY FAILED → OK → ENABLE → OK

Battery dead or missing/battery connection restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → ENABLE → OK

Test event: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → TEST EVENT → OK → ENABLE → OK

Tamper alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → TAMPER ALM/REST EV → OK → ENABLE → OK

Panic/Silent zone alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → PA/SIL ALM/REST EV → OK → ENABLE → OK

System started: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → SYSTEM STARTED EV → OK → ENABLE → OK

Fire alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → FIRE ALM/REST EV → OK → ENABLE → OK

24-Hour zone alarm/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → 24H ALM/REST EVENT→ OK → ENABLE → OK

Low battery: OK → iiii → OK → MS SETTINGS → OK →DATA MESSAGES 1 → OK → LOW BATTERY EVENT → OK → ENABLE → OK

Temperature risen: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → TEMP HIGH EVENT → OK → ENABLE → OK

Temperature fallen: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → TEMP LOW EVENT → OK → ENABLE → OK

Wireless signal loss/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 1 → OK → WLESS SIGN L/R EV → OK → ENABLE → OK

Disarmed by user (Duress code): OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → DISARM DURESS EV → OK → ENABLE → OK

Armed/disarmed by user (SGS code): OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → ARM/DARM SGS EVENT → OK → ENABLE → OK

Armed/disarmed in Stay mode: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → ARM/DARM STAY EV → OK → ENABLE → OK

Siren fail/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → SIREN FAIL/REST EV → OK → ENABLE → OK

Date/time not set: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → DATE/TIME NOT SET → OK → ENABLE → OK

GSM connection failed: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → GSM CONNECT FAILED → OK → ENABLE → OK

GSM/GPRS antenna fail/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → ENABLE → OK

System shutdown: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → SYSTEM SHUTDOWN EV → OK → ENABLE → OK

Keypad fail/restore: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → KEYPAD FAIL/REST → OK → ENABLE → OK

GPRS connection failed: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → GPRS CONNECT FAIL → OK → ENABLE → OK

Zone bypassed/activated: OK → iiii → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → ZONE BYPASS→ OK → ENABLE → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 24, event number & parameter status value:

24 01 1 # – Burglary alarm/restore

24 02 1 # – Mains power loss/restore

24 03 1 # – Armed/disarmed by user

24 04 1 # – Test event

24 05 1 # – Battery failed

24 06 1 # – Battery dead or missing/battery connection restore

24 07 1 # – Tamper alarm/restore

24 08 1 # – Panic/Silent zone alarm/restore

24 09 1 # – Kronos ping

24 10 1 # – System started

24 13 1 # – 24-Hour zone alarm/restore

24 14 1 # – Fire zone alarm/restore

24 15 1 # – Low battery

24 16 1 # – Temperature risen

24 17 1 # – Temperature fallen

24 18 1 # – Wireless signal loss/restore

24 19 1 # – Disarmed by user (Duress code)

24 20 1 # – Armed/disarmed by user (SGS code)

24 21 1 # – Armed/disarmed in Stay mode

24 22 1 # – Siren fail/restore

24 24 1 # -Date/time not set

24 25 1 # – GSM connection failed

24 26 1 # – GSM/GPRS antenna fail/restore

24 27 1 # – System shutdown

24 28 1 # – Keypad fail/restore

24 29 1 # – GPRS connection failed

24 30 1 # – Zone bypassed/activated

Example: *24031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

30.2. Communication

The system supports the following communication methods and protocols:

- GPRS network – EGR100, Kronos, SIA IP protocol.
- Voice calls (GSM audio channel) – Ademco Contact ID protocol.
- RS485 data channel.
- CSD (Cricuit Switched Data).
- PSTN (landline) – Ademco Contact ID protocol.
- SMS – Cortex SMS format.
- ELAN3-ALARM – EGR100, Kronos, SIA IP protocol.

Any communication method can be set as primary or backup connection. The user can set up to 5 backup connections in any sequence order.

Initially, the system communicates via primary connection with the monitoring station. By default, if the initial attempt to transmit data is unsuccessful, the system will make additional attempts until the data is successfully delivered. If all attempts are unsuccessful, the system will follow this pattern:

a) The system switches to the backup connection that follows in the sequence (presumably - Backup 1).

b) The system then attempts to transmit data by the backup connection.

c) If the initial attempt is unsuccessful, the system will make additional attempts until the data is successfully delivered.

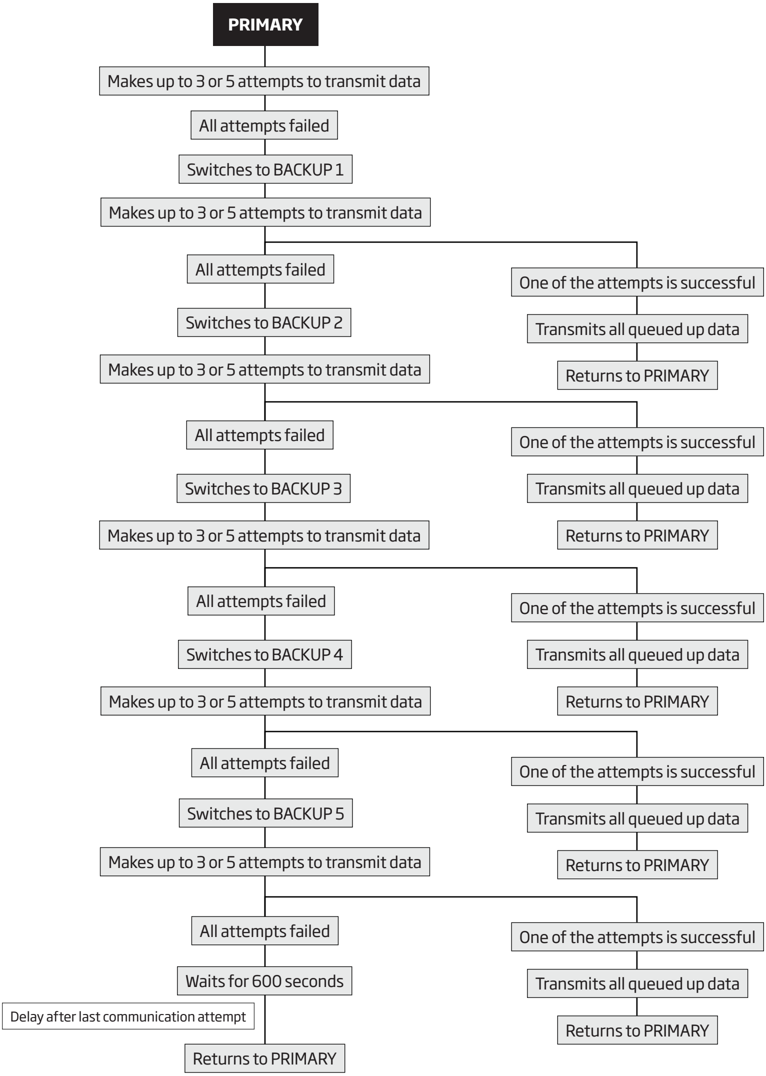
d) If the system ends up with all unsuccessful attempts, it will switch to the next backup connection in the sequence (presumably - Backup 2) and will continue to operate as described in the previous steps. The connection is considered unsuccessful under the following conditions:
   - GPRS network/ELAN3-ALARM – The system has not received the ACK data message from the monitoring station within 40 seconds.
   - Voice calls:
     - The system has not received the “handshake” signal from the monitoring station within 40 seconds.
     - The system has not received the “kissoff” signal from the monitoring station within 5 attempts each lasting 1 second.
   - CSD – The system has not received the ACK data message from the monitoring station within 35 seconds.
   - PSTN:
     - The system has not received the “handshake” signal from the monitoring station within 40 seconds.
     - The system has not received the “kissoff” signal from the monitoring station within 5 attempts each lasting 1 second.
   - SMS – The system has not received the SMS delivery report from the SMSC (Short Message Service Center) within 45 seconds.

e) If one of the attempts is successful, the system will transmit all queued up data messages by this connection.

f) The system then returns to the primary connection and attempts to transmit the next data messages by primary connection.

g) If the system ends up with all unsuccessful attempts by all connections, it will wait until the *Delay after last communication attempt* time (By default – 600 seconds) expires and will return to the primary connection afterwards.

h) If a new data message, except Test Event (ping), is generated during *Delay* after last communication attempt time, the system will immediately attempt to transmit it to the monitoring station, regardless of *Delay* after last communication attempt being in progress.


PRIMARY
Makes up to 3 or 5 attempts to transmit data
All attempts failed
Switches to BACKUP 1
Makes up to 3 or 5 attempts to transmit data
All attempts failed
One of the attempts is successful
Switches to BACKUP 2
Transmits all queued up data
Makes up to 3 or 5 attempts to transmit data
Returns to PRIMARY
All attempts failed
One of the attempts is successful
Switches to BACKUP 3
Transmits all queued up data
Makes up to 3 or 5 attempts to transmit data
Returns to PRIMARY
All attempts failed
One of the attempts is successful
Switches to BACKUP 4
Transmits all queued up data
Makes up to 3 or 5 attempts to transmit data
Returns to PRIMARY
All attempts failed
One of the attempts is successful
Switches to BACKUP 5
Transmits all queued up data
Makes up to 3 or 5 attempts to transmit data
Returns to PRIMARY
All attempts failed
One of the attempts is successful
Waits for 600 seconds
Transmits all queued up data
Delay after last communication attempt
Returns to PRIMARY
Returns to PRIMARY

NOTE: The number of attempts, indicated in the diagram, are default and depends on the determined communication method.

NOTE: When using Dual-SIM feature, the Secondary SIM card is involved in the communication process. For more details, please refer to **31. DUAL SIM MANAGEMENT.**

Set primary connection

EKB2

Menu path:

GPRS network: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → GPRS → OK

Voice calls: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → VOICE CALLS → OK

RS485: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → RS485 → OK

CSD: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → CSD → OK

PSTN: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → PSTN → OK

SMS: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → SMS → OK

ELAN3-ALARM: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → ELAN3-ALARM → OK

connection not in use: OK → iiii → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → N/A → OK

Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 48 & communication method number:

48 0 # – GPRS network

48 1 # – Voice calls

48 2 # – RS485

48 3 # – CSD

48 4 # – PSTN

48 5 # – SMS

48 6 # – ELAN3-ALARM

48 7 # – connection not in use

Example: 484#

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set backup connection 1... 5

EKB2

Menu path:

GPRS network: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → GPRS → OK

Voice calls: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → VOICE CALLS → OK

RS485: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → RS485 → OK

CSD: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → CSD → OK

PSTN: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → PSTN → OK

SMS: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → SMS → OK

ELAN3-ALARM: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → ELAN3-ALARM → OK

connection not in use: OK → iiii → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 5 → OK → N/A → OK

Value: iiii – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 83, backup connection slot number & communication method number:

83 bb 0 # – GPRS network

83 bb 1 # – Voice calls

83 bb 2 # – RS485

83 bb 3 # – CSD

83 bb 4 # – PSTN

83 bb 5 # – SMS

83 bb 6 # – ELAN3-ALARM

83 bb 7 # – connection not in use

Value: *bb* – backup con

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If all attempts by all set connections are unsuccessful, the system will wait until the delay time (By default – 600 seconds) expires and will attempt to transmit data to the monitoring station again starting with the primary connection.

Set delay after last communication attempt

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → DELAY LAST ATTEMPT → OK → aaapp → OK
Value: *iiii* – 4-digit installer code; *aaapp* – duration of delay after last attempt, range – [0... 65535] seconds.

EKB3/ EKB3W

Enter parameter 69 & duration of delay after last attempt:
69 aaapp #
Value: *aaapp* – duration of delay after last attempt, range – [0... 65535] seconds.
Example: *69200#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: 0 value disables delay after last communication attempt.

NOTE: The system is fully compatible with Kronos NET/Kronos LT monitoring station software for communication via GPRS network. When using a different monitoring station software, EGR100 middleware is required. EGR100 is freeware and can be downloaded at www.eldes.lt/en/download

30.2.1. GPRS Network and ELAN3-ALARM

The system supports data transmission to the monitoring station via IP-based networks by GPRS network or Ethernet connection using ELAN3-ALARM device (see **32.1.4. ELAN3-ALARM - Ethernet Communicator**). The supported data formats are the following:

- EGR100
- Kronos
- SIA IP

To set up the system for data transmission via GPRS network or Ethernet using ELAN3-ALARM, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Account number (see **30. MONITORING STATION**).
3. Set server IP address, which is a public IP address of the machine running EGR100, Kronos or SIA IP-based monitoring station software.
4. Set server port, which is a port of the machine running EGR100, Kronos or SIA IP-based monitoring station software.
5. Select TCP or UDP protocol. UDP is highly recommended for EGR100 and SIA IP data format.
6. Select data format: EGR100, Kronos or SIA IP.
7. In case EGR100 is selected, set 4-digit Unit ID number. Unit ID number can be identical to Account number.
8. When using GPRS network connection, it is necessary to set up APN, user name and password provided by the GSM operator. Depending on the GSM operator, only APN might be required to set up.

For detailed step-by-step instructions on how to establish the communication between ESIM364 alarm system and EGR100 middleware, please refer to the middleware's HELP file.

Set server IP address

SMS

SMS text message content:
ssss_SETGPRS:IP:add.add.add.add
Value: *ssss* – 4-digit SMS password; *add.add.add.add* – server IP address.
Example: *1111_SETGPRS:IP:65.82.119.5*

EKB2

Menu path:
OK → iiii → OK → GPRS SETTINGS → OK → SERVER IP → OK → add.add. add.add → OK
Value: *iiii* – 4-digit installer code; *add.add.add.add* – server IP address.

EKB3/ EKB3W

Enter parameter 40 & server IP address:
40 add add add add #
Value: *add add add add* – server IP address.
Example: *40065082119005#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set server port

SMS

SMS text message content:
ssss_SETGPRS:PORT:pprrt
Value: *ssss* – 4-digit SMS password; *pprrt* – server port number, range – [1... 65535].
Example: *1111_SETGPRS:PORT:5521*

EKB2

Menu path:
OK → iiii → OK → GPRS SETTINGS → OK → SERVER PORT → OK → pprrt → OK
Value: *iiii* – 4-digit installer code; *pprrt* – server port number, range – [1... 65535].

EKB3/ EKB3W

Enter parameter 44 & server port number:
44 pprrt #
Value: *pprrt* – server port number, range – [1... 65535].
Example: *443365#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set DNS1 server IP address

EKB2

Menu path:
OK → iiii → OK → GPRS SETTINGS → OK → DNS1 → OK → add. add.add. add → OK
Value: *iiii* – 4-digit installer code; *add.add.add.add* – DNS1 server IP address.

EKB3/ EKB3W

Enter parameter 41 & DNS1 server IP address:
41 add add add add #
Value: *add add add add* – DNS1 server IP address.
Example: *41065082119001#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set DNS2 server IP address

EKB2

Menu path:
OK → iiii → OK → GPRS SETTINGS → OK → DNS2 → OK → add. add.add. add → OK
Value: *iiii* – 4-digit installer code; *add.add.add.add* – DNS2 server IP address.

EKB3/ EKB3W

Enter parameter 42 & DNS2 server IP address:
42 add add add add #
Value: *add add add add* – DNS2 server IP address.
Example: *41065082119002#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set protocol

SMS

SMS text message content:
ssss_SETGPRS:PROTOCOL:ptc
Value: *ssss* – 4-digit SMS password; *ptc* – protocol, range – [TCP... UDP].
Example: *1111_SETGPRS:PROTOCOL:UDP*

EKB2

Menu path:
OK → iiii → OK → GPRS SETTINGS → OK → PROTOCOL → OK → TCP | UDP → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 43 & protocol number:
430# - TCP
431# - UDP
Example: *431#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set data format as Kronos, EGR100 or SIA IP

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Manage SIA IP data format parameters

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Kronos NET/Kronos LT software communicates via TCP protocol, while EGR100 middle-ware v1.2 and up supports both – TCP and UDP protocols. However, TCP protocol is NOT recommend to use with EGR100.

ATTENTION: It is necessary to restart the system locally by powering down and powering up the system the system or remotely (see **35. REMOTE SYSTEM RESTART**) after changing the IP address or switching from TCP to UDP.

By default, if the initial attempt to transmit data to the monitoring station via GPRS network or Ethernet method is unsuccessful, the system will make up to 2 additional attempts. If all attempts are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → IP SETTINGS → OK → IP ATTEMPTS → OK → att → OK
Value: *iiii* – 4-digit installer code; *att* – number of attempts, range – [1... 255].

EKB3/ EKB3W

Enter parameter 68 & number of attempts:
68 att #
Value: *att* – number of attempts, range – [01... 255].
Example: *6809#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To report the online status, the system periodically transmits (By default – every 180 seconds) Test Event data message (ping) to the monitoring station via GPRS network or Ethernet.

Set test period

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → IP SETTINGS → OK → TEST PERIOD → OK → tteessttpp → OK
Value: *iiii* – 4-digit installer code; *tteessttpp* – test period, range – [0... 65535] seconds.

EKB3/ EKB3W

Enter parameter 46 & number of attempts:
46 tteessttpp #
Value: *tteessttpp* – test period, range – [0... 65535] seconds.
Example: *46120#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: 0 value disables test period.

Unit ID is a 4-digit number (By default - 0000) required to identify the alarm system unit by EGR100 middle-ware. It is MANDATORY to change the default Unit ID before using EGR100.

Set unit ID

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → IP SETTINGS → OK → UNIT ID → OK → unid → OK
Value: *iiii* - 4-digit installer code; *unid* - 4-digit unit ID number.

EKB3/ EKB3W

Enter parameter 47 & unit ID number:
47 unid #
Value: *unid* - 4-digit unit ID number.
Example: *472245#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For communication via GPRS network, the GPRS parameters provided by the GSM operator are necessary to be set up. To set those parameters, please refer to the following configuration methods.

Set APN

SMS

SMS text message content:
ssss_SETGPRS:APN:acc-point-name
Value: *ssss* - 4-digit SMS password; *acc-point-name* - up to 31 character APN (Access Point Name) provided by the GSM operator.
Example: *1111_SETGPRS:APN:internet*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set user name

SMS

SMS text message content:
ssss_SETGPRS:USER:usr-name
Value: *ssss* - 4-digit SMS password; *usr-name* - up to 31 character user name provided by the GSM operator.
Example: *1111_USER:mobileusr*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set password

SMS

SMS text message content:
ssss_SETGPRS:PSW:password
Value: *ssss* - 4-digit SMS password; *password* - up to 31 character password provided by the GSM operator.
Example: *1111_SETGPRS:PSW:mobilepsw*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View IP and GPRS network settings

SMS

SMS text message content:
ssss_SETGPRS?
Example: *1111_SETGPRS?*

EKB2

Menu path:
Server IP: OK → iiii → OK → GPRS SETTNGS → OK → IP SETTINGS → OK → SERVER IP
Server port: OK → iiii → OK → GPRS SETTNGS → OK → PORT
DNS1: OK → iiii → OK → GPRS SETTNGS → OK → DNS1
DNS2: OK → iiii → OK → GPRS SETTNGS → OK → DNS2
Protocol: OK → iiii → OK → GPRS SETTNGS → OK → PROTOCOL
DNS1: OK → iiii → OK → GPRS SETTNGS → OK → DNS1
APN: OK → iiii → OK → GPRS SETTINGS → OK → APN
User name: OK → iiii → OK → GPRS SETTINGS → OK → USERS
Password: OK → iiii → OK → GPRS SETTINGS → OK → PASSWORD
Value: *iiii* – 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

30.2.2. Voice Calls and SMS

The system supports up to 3 monitoring station phone numbers for communication with the alarm system by Voice Calls or SMS communication method using Ademco Contact ID or Cortex SMS data format respectively. Tel. Number 1 is mandatory, the other two can be used as backup phone numbers and are not necessary. The supported phone number formats are the following:

- **International (with plus)** – The phone numbers must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for *UK: +4417091111111*. This format can be used when setting up the phone number by *ELDES Configuration Tool* software.
- **International (with 00)** – The phone numbers must be entered starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for *UK: 004417091111111*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad.
- **Local** – The phone numbers must be entered starting with an area code in the following format: [area code][local number], example for *UK: 017091111111*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software.

To set up the system for data transmission via Voice Calls or SMS, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Account number (see **30. MONITORING STATION**).
3. Set Tel. Number 1... 3.

Set monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → TEL. NUMBER 1... 3 → OK → ttteeellnnuumm → OK
Value: *iiii* – 4-digit installer code; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.

EKB3/ EKB3W

Enter parameter 26, phone number slot & phone number:
26 ps ttteeellnnuumm #
Value: *ps* – phone number slot, range – [01... 03]; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.
Example: *2601004417091111111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → TEL. NUMBER 1... 3 → OK → OK
Value: *iiii* – 4-digit installer code..

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station's Tel Number 1 via Voice Calls or SMS method is unsuccessful, the system will make up to 4 additional attempts. After all unsuccessful attempts, the system will continue to communicate with the monitoring station by switching to the next phone number that follows in the sequence and making up to 4 additional attempts if the initial attempt is unsuccessful. If all attempts to all phone numbers are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → ATTEMPTS → OK → at → OK
Value: *iiii* – 4-digit installer code; *at* – number of attempts, range – [1... 10].

EKB3/ EKB3W

Enter parameter 37 & number of attempts:
37 at #
Value: *at* – number of attempts, range – [01... 10].
Example: *3706#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Due to the individual configuration of each monitoring station, the system may fail to deliver the data message via Voice Calls communication method. In such cases it is recommended to adjust the microphone gain until the optimal value, leading to successful data message delivery, is discovered.

Set microphone gain

EKB2

Menu path:
OK → iiii → OK → PRIMARY SETT INGS → OK → GSM AUDIO → OK → MICROPHONE GAIN → OK → mg → OK
Value: *iiii* – 4-digit installer code; mg – microphone gain, range – [0... 15].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

30.2.3. PSTN

The system supports up to 3 monitoring station phone numbers for communication with the alarm system by PSTN communication method using Ademco Contact ID data format. Tel. Number 1 is mandatory, the other two can be used as backup phone numbers and are not necessary. The supported phone number formats are the following:

- **International (with 00)** – The phone numbers must be entered starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for *UK: 004417091111111*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software..
- **Local** – The phone numbers must be entered starting with an area code in the following format: [area code][local number], example for *UK: 017091111111*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software.

To set up the system for data transmission via Voice Calls or SMS, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Account number (see **30. MONITORING STATION**).
3. Set Tel. Number 1... 3.

Set monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → PSTN SETTINGS → OK → TEL. NUMBER 1... 3 → OK → ttteeellnnuumm → OK
Value: *iiii* – 4-digit installer code; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.

EKB3/ EKB3W

Enter parameter 58, phone number slot & phone number:
58 ps ttteeellnnuumm #
Value: *ps* – phone number slot, range – [01... 03]; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.
Example: *5802004417091111111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete monitoring station phone number

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → PSTN SETTINGS → OK → TEL. NUMBER 1... 3 → OK → OK
Value: *iiii* – 4-digit installer code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station's Tel Number 1 via PSTN method is unsuccessful, the system will make up to 4 additional attempts. After all unsuccessful attempts, the system will switch to the next phone number that follows in the sequence and will make up to 4 additional attempts if the initial attempt is unsuccessful. If all attempts to all phone numbers are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → iiii → OK → MS SETTINGS → OK → PSTN SETTINGS → OK → ATTEMPTS → OK → at → OK
Value: *iiii* – 4-digit installer code; *at* – number of attempts, range – [1... 10].

EKB3/ EKB3W

Enter parameter 91 & number of attempts:
91 at #
Value: *at* – number of attempts, range – [01... 10].
Example: *9108#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Alternatively, the phone number entries can be treated as phone numbers for receiving calls in case of alarm. For more details on how this method operates, please refer to **17. ALARM INDICATIONS AND NOTIFICATIONS**

To enable/disable this feature, please refer to the following configuration method.

Enable/disable Treat PSTN Call as User Call

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

30.2.4. CSD

The system supports up to 5 monitoring station phone numbers for communication with the alarm system by CSD communication method. Tel. Number 1 is mandatory, the other four can be used as backup phone numbers and are not necessary. The supported phone number formats are the following:

- **International (with plus)** – The phone number must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for *UK: +4417091111111*. This format can be used when setting up the phone number by *ELDES Configuration Tool* software.
- **International (with 00)** – The phone number must be entered starting with 00 and an international country code in the following ž format: 00[international code][area code][local number], example for *UK: 004417091111111*. This format can be used when setting up the phone number by EKB2/EKB3/EKB3W keypad.

To set up the system for data transmission via CSD, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Account number (see **30. MONITORING STATION**).
3. Set Tel. Number 1... 5.

Set monitoring station phone number

EKB2 **Menu path:**
OK → iiii → OK → MS SETTINGS → OK → CSD SETTINGS → OK → TEL. NUMBER 1... 5 → OK → ttteeellnnuumm → OK
Value: *iiii* – 4-digit installer code; ttteeellnnuumm – up to 15 digits monitoring station phone number.

EKB3/ EKB3W **Enter parameter 85, number of entry & phone number:**
85 ps ttteeellnnuumm #
Value: *ps* – phone number slot, range – [01... 05]; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.
Example: *8501004417091111111#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete monitoring station phone number

EKB2 **Menu path:**
OK → iiii → OK → MS SETTINGS → OK → CSD SETTINGS → OK → TEL. NUMBER 1... 5 → OK → OK
Value: *iiii* – 4-digit installer code.

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station's phone number via CSD method is unsuccessful, the system will make up to 4 additional attempts. If all attempts are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2 **Menu path:**
OK → iiii → OK → MS SETTINGS → OK → CSD SETTINGS → OK → ATTEMPTS → OK → at → OK
Value: *iiii* – 4-digit installer code; *at* – number of attempts, range – [1... 10].

EKB3/ EKB3W **Enter parameter 84 & number of attempts:**
84 at #
Value: *at* – number of attempts, range – [01... 10].
Example: *8403#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

31. DUAL SIM MANAGEMENT

The Dual-SIM feature allows the system to operate with one of the two inserted SIM cards identified as Primary SIM and Secondary SIM respectively. The Primary SIM card works as the main default card, while the Secondary SIM card is intended for backup purposes or addition to the Primary SIM card - SMS text message sending/calling to the preset user phone number and/or communication with the monitoring station.

The Dual-SIM feature can operate in one of the following modes:

- **Disabled** – The Secondary SIM card will not be functional and the system operates with Primary SIM card only (by default – enabled).
- **Automatic** – The system switches between the SIM cards in case of a GSM connection or one of the SIM cards failure.
- **Manual** – Provides a fully customizable set up of switching between the SIM cards. FOR ADVANCED USERS ONLY!

Manage Dual -SIM feature

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Regardless of the selected mode, only one of the two SIM cards can operate at the same time.

NOTE: The Dual-SIM feature becomes automatically disabled when the Smart Security feature is in use.

31.1. Disabled Mode

Disabled mode is the default system mode that does not involve the Secondary SIM in the communication process. When this mode is in use, the system will ignore the Secondary SIM card even if inserted in the SIM card slot.

For more details on how the system communicates with the user and the monitoring station in Disabled mode, please refer to **17. ALARM INDICATIONS AND NOTIFICATIONS** and **30.2. Communication** respectively.

31.2. Automatic Mode

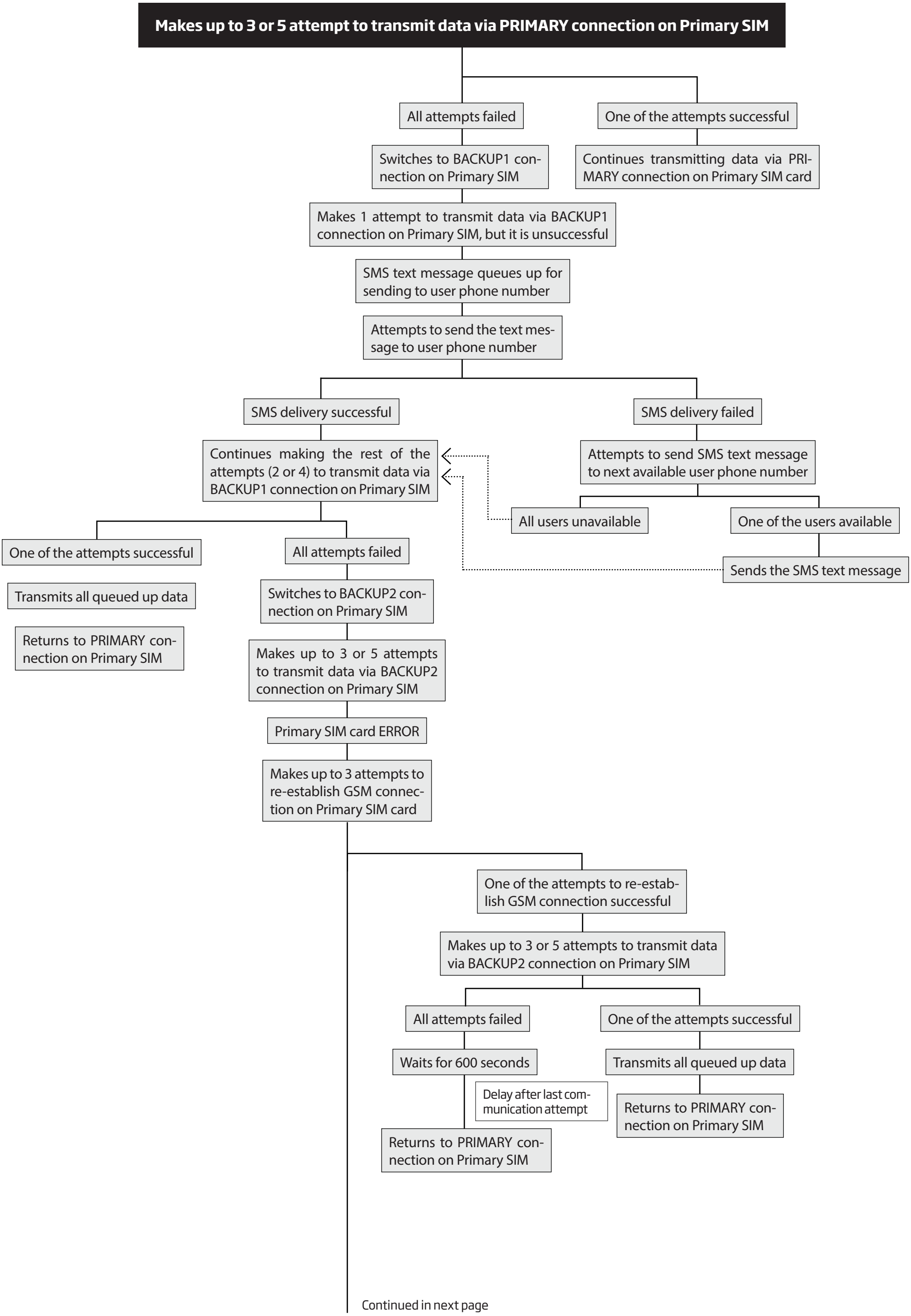
Automatic mode involves both SIM cards in the communication process. In this mode there is no Primary or Secondary SIM card hierarchy, since both cards are equal and the SIM card that is currently in use maintains the GSM connection at all time, unless a failure occurs and the other card would replace the previous one.

When one of the SIM card fails, the system attempts to re-establish a connection with it by starting an initial reconnection for a set number of attempts (by default - 3 attempts). If all attempts fail, the system will switch to the other SIM card. If the other SIM card is responsive and a GSM connection is successfully established, the system will remain operating with that SIM card until it fails. However, if the other SIM card is unresponsive or it is not present in the SIM card slot, the system will return to the previous SIM card and attempt to establish a GSM connection with it. If the system fails to carry out this action, after a single attempt it will switch to the other SIM card. This cycle continues until one of the SIM cards responds and a GSM connection is successfully established. When the SIM card fails, the system will once again attempt to restore the GSM connection for a set number of attempts (by default – 3 attempts). If all attempts fail, the cycle will continue as described previously.

In Automatic mode the priority is to transmit data to the monitoring station, but if an event, which requires the system to send an SMS text message occurs , the system will send the SMS text message via the SIM card that is currently in use. This can only be carried out under the following conditions:

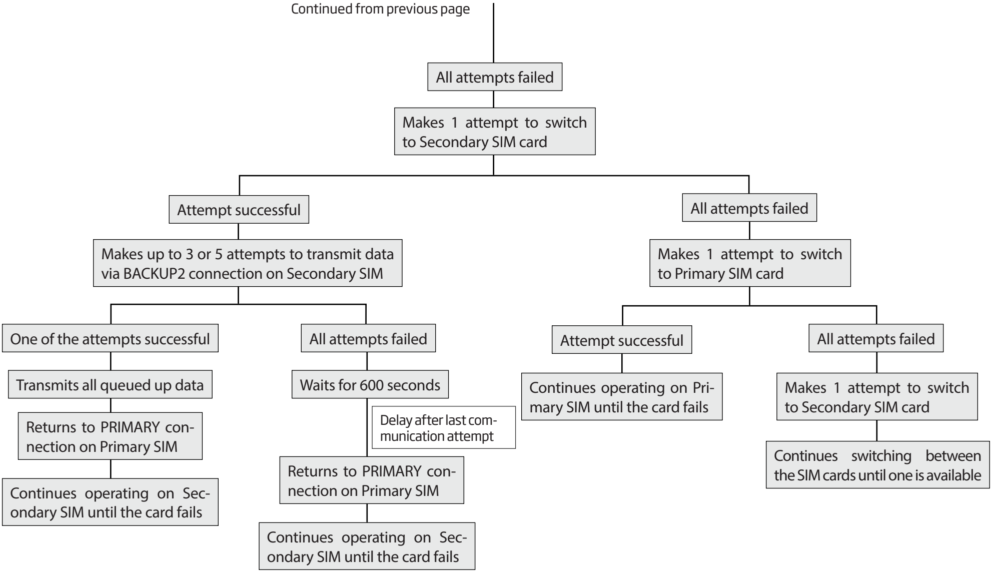
- among the attempts to transmit data to the monitoring station (depending on communication method).
- while switching the monitoring station connections.
- while switching between the SIM cards.

The following example indicates the situation described above.


Makes up to 3 or 5 attempt to transmit data via PRIMARY connection on Primary SIM
All attempts failed
One of the attempts successful
Switches to BACKUP1 connection on Primary SIM
Continues transmitting data via PRIMARY connection on Primary SIM card
Makes 1 attempt to transmit data via BACKUP1 connection on Primary SIM, but it is unsuccessful
SMS text message queues up for sending to user phone number
Attempts to send the text message to user phone number
SMS delivery successful
SMS delivery failed
Continues making the rest of the attempts (2 or 4) to transmit data via BACKUP1 connection on Primary SIM
Attempts to send SMS text message to next available user phone number
All users unavailable
One of the users available
Sends the SMS text message
One of the attempts successful
All attempts failed
Transmits all queued up data
Returns to PRIMARY connection on Primary SIM
Switches to BACKUP2 connection on Primary SIM
Makes up to 3 or 5 attempts to transmit data via BACKUP2 connection on Primary SIM
Primary SIM card ERROR
Makes up to 3 attempts to re-establish GSM connection on Primary SIM card
One of the attempts to re-establish GSM connection successful
Makes up to 3 or 5 attempts to transmit data via BACKUP2 connection on Primary SIM
All attempts failed
One of the attempts successful
Waits for 600 seconds
Delay after last communication attempt
Transmits all queued up data
Returns to PRIMARY connection on Primary SIM
Returns to PRIMARY connection on Primary SIM

Continued in next page

Continued from previous page


All attempts failed
Makes 1 attempt to switch to Secondary SIM card
Attempt successful
All attempts failed
Makes up to 3 or 5 attempts to transmit data via BACKUP2 connection on Secondary SIM
Makes 1 attempt to switch to Primary SIM card
One of the attempts successful
All attempts failed
Attempt successful
All attempts failed
Transmits all queued up data
Waits for 600 seconds
Continues operating on Primary SIM until the card fails
Makes 1 attempt to switch to Secondary SIM card
Delay after last communication attempt
Returns to PRIMARY connection on Primary SIM
Continues switching between the SIM cards until one is available
Returns to PRIMARY connection on Primary SIM
Continues operating on Secondary SIM until the card fails
Continues operating on Secondary SIM until the card fails

NOTE: The number of attempts, indicated in the diagram, are default and depends on the determined communication method

31.3. Manual Mode

Manual mode allows to use both - Primary and Secondary SIM cards and fully customize the algorithm of the communication. The system can be set up to send SMS text messages/call to the preset user phone number and/or communicate with the monitoring station as follows:

- **Primary SIM** – Determines that the SMS text messages/calls/data will be transmitted via the Primary SIM card.
- **Secondary SIM** – Determines that the SMS text messages/calls/data will be transmitted via the Secondary SIM card.
- **Currently in use SIM** – Determines that the SMS text messages/calls/data will be transmitted via the SIM card that the system is currently switched to - either Primary or the Secondary SIM card.
- **Return to Primary SIM Enabled** – Determines that the Primary SIM card will be the main SIM card of the system. If it is set up to use the Secondary SIM in the communication process, the system will do so, but after completing the task via the Secondary SIM card, the system will always return to the Primary SIM card
- **Try to find operator for a maximum of x times** – Determines the maximum number of attempts the system should attempt to re-establish a GSM connection on the current SIM card in case of unsuccessful initial attempt (by default – 3 attempts).

In Manual mode the priority is to transmit data to the monitoring station, but if an event, which requires the system to send an SMS text message via one of the SIM cards, occurs , the system will switch to the requested SIM card and send the SMS text message. This can only be carried out under the following conditions:

- among the attempts to transmit data to the monitoring station (depending on communication method).
- while switching the monitoring station connections.
- while switching between the SIM cards.

Example: System settings are the following:

Dual SIM Management:

- **Manual Mode** selected
- **Return to Primary SIM** – Disabled.
- **Send SMS / Call via** – Secondary SIM.

MS Settings – Communication:

- **Primary** – Voice Calls via Secondary SIM.
- **Backup1** – CSD via Primary SIM.
- **Backup2** – GPRS Network via Primary SIM.

Let's say, the system is configured to send an SMS text message to user phone number in case of a Fire Zone Alarm and to transmit data to the monitoring station when the system is ARMED. The system is currently switched to the Primary SIM card. The system will follow this pattern:

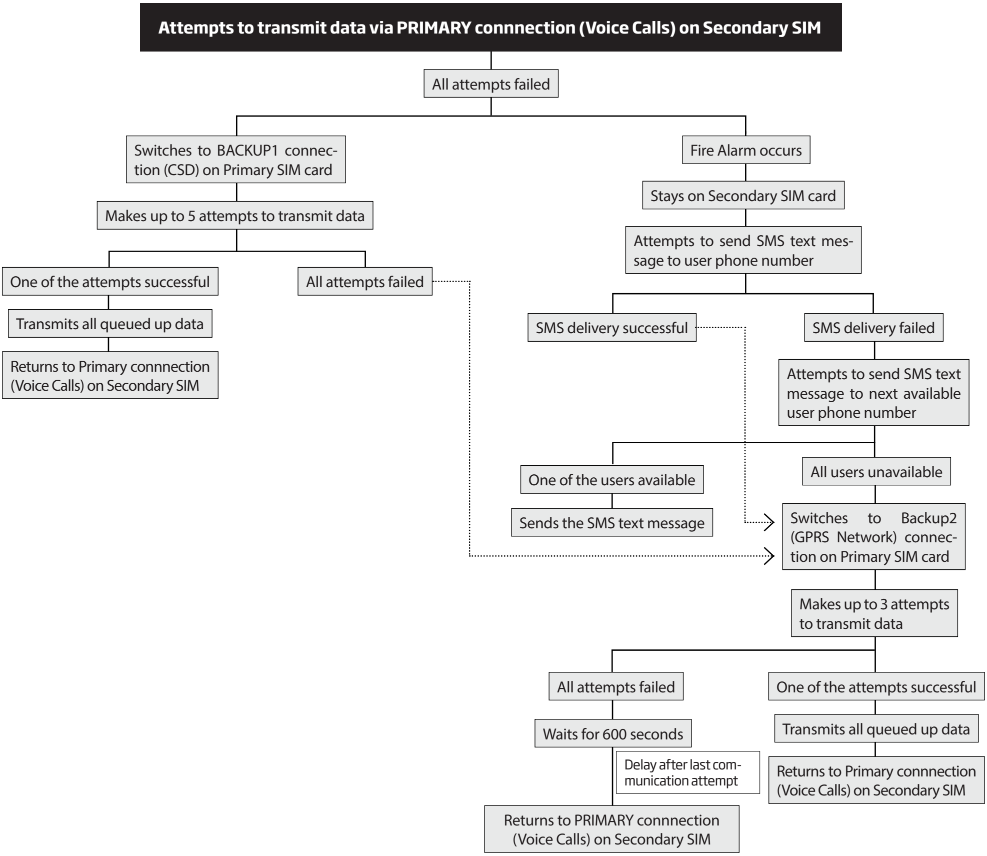
a) The user arms the system followed by system switching to the Secondary SIM and attempting to transmit data to the monitoring station via the Primary connection, which is Voice Calls communication method, but fails.

b) The system then switches to the Primary SIM and attempts to transmit data via Backup1 connection, which is CSD communication method, but fails again.

c) During the event described in step b), a Fire Zone Alarm occurs. The system will switch to the Secondary SIM and attempt to send the SMS text message to the user regarding this event.

d) The system continues with the data transmission to the monitoring station by switching back to Primary SIM and attempting to transmit data via Backup2 connection, which is GPRS Network communication method, and succeeds.

e) The alarm system switches back to the Primary connection (Voice Calls) and to the Secondary SIM card and waits until the occurrence of further events.


Attempts to transmit data via PRIMARY connnection (Voice Calls) on Secondary SIM
All attempts failed
Switches to BACKUP1 connection (CSD) on Primary SIM card
Makes up to 5 attempts to transmit data
One of the attempts successful
Transmits all queued up data
Returns to Primary connnection (Voice Calls) on Secondary SIM
All attempts failed
Fire Alarm occurs
Stays on Secondary SIM card
Attempts to send SMS text message to user phone number
SMS delivery successful
SMS delivery failed
Attempts to send SMS text message to next available user phone number
One of the users available
Sends the SMS text message
All users unavailable
Switches to Backup2 (GPRS Network) connection on Primary SIM card
Makes up to 3 attempts to transmit data
All attempts failed
Waits for 600 seconds
Delay after last communication attempt
Returns to PRIMARY connnection (Voice Calls) on Secondary SIM
One of the attempts successful
Transmits all queued up data
Returns to Primary connnection (Voice Calls) on Secondary SIM

NOTE: The number of attempts, indicated in the diagram, are default and depends on the determined communication method

NOTE: If the Return to Primary SIM parameter is enabled, the system would return to the Primary SIM after each data transmission.

32. ELDES WIRED DEVICES

32.1. RS485 Interface

RS485 interface is used for the system to communicate with the following devices:

- EKB2 keypads (up to 4 units).
- EKB3 keypads (up to 4 units).
- EPGM1 modules (up to 2 units).
- ELAN3-ALARM (1 unit)

The terminals of RS485 interface are Y (yellow wire) and G (green wire), which are clock and data respectively. The devices, connected to RS485 interface, must be powered from the AUX+ and AUX- terminals.

For more details on RS485 device wiring, please refer to **3.2.7. RS485**.

32.1.1. EKB2 - LCD Keypad

EKB2 is an LCD keypad intended for using with ESIM364 alarm system.

Main EKB2 features:

- Alarm system arming and disarming (see **12.3. EKB2 Keypad and User Password**).
- Arming and disarming in Stay mode (see **15. STAY MODE**).
- System parameter configuration (see **5. CONFIGURATION METHODS**).
- PGM output control (see **18.4. Turning PGM Outputs ON and OFF**).
- System information display (see **32.1.1.4. Visual and Audio Indications**).
- Audio indication by built-in buzzer (see **32.1.1.4. Visual and Audio Indications**).
- Wireless device information display (see **19.2. Wireless Device Information and Signal Status Monitoring**).
- Temperature display (see **32.1.1.1.2 Keys Functionality**).
- Time display (see **32.1.1.1.2 Keys Functionality**).

The system configuration is performed by accessing EKB2 menu and entering the required values. ESIM364 system allows to connect up to 4 EKB2 keypads.

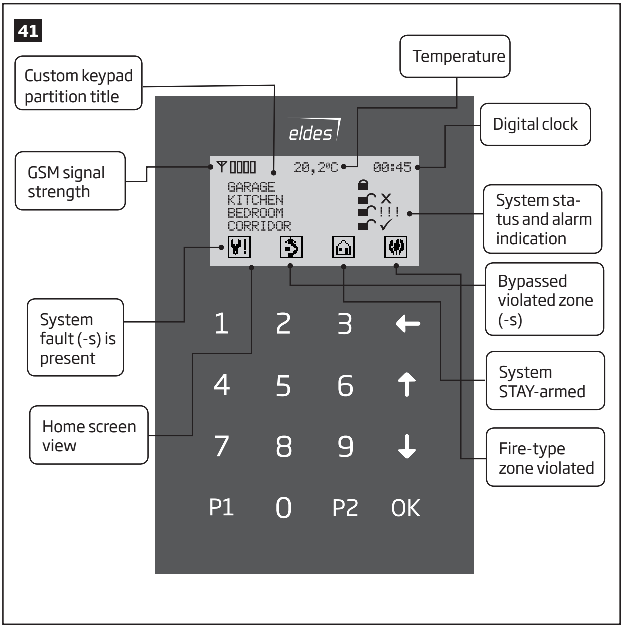
32.1.1.1. Technical Specifications

32.1.1.1.1 Electrical & Mechanical Characteristics

Power supply	12-14V ⎓ 150mA max.
Maximum keypad connection cable length	100 m.
Dimensions	133 x 89 x 19 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Range of operating temperatures	0...+55°C

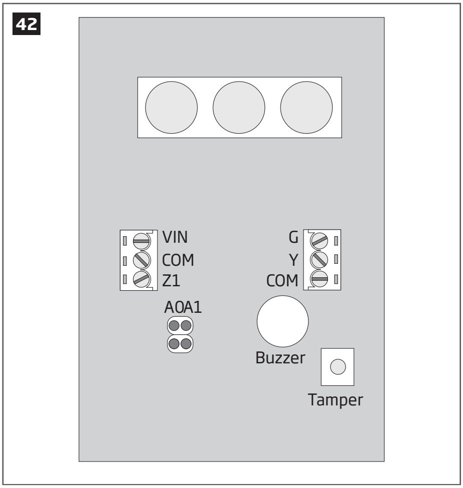
32.1.1.1.2 Keys Functionality

←	One menu level back / cancel
↑	Menu navigation – up
↓	Menu navigation – down
OK	Confirm (enter) value
0 ... 9	Value typing
P1	Minus character to enter negative temp. value
P2	Additional menu / minus character to enter negative temp. value


41

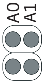
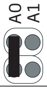
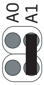
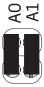
32.1.1.1.3 Connector and Main Unit Functionality

Vin	Positive power supply terminal
COM	Negative power supply terminal
G	RS485 interface for communication (green wire)
Y	RS485 interface for communication (yellow wire)
COM	Common terminal for Z1
Z1	Security zone terminal
A0	Keypad address pin
A1	Keypad address pin
Buzzer	Buzzer for audio indications
Tamper	Tamper-button for EKB2 enclosure status monitoring


42

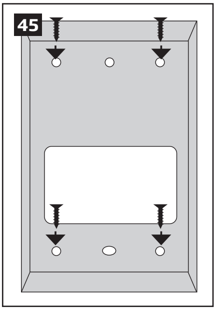
32.1.1.1.4 Keypad Address

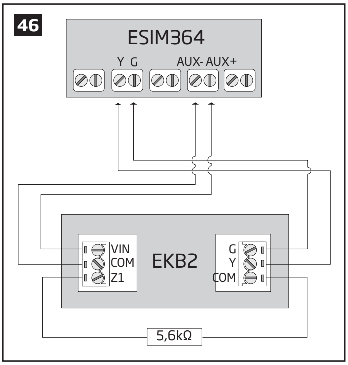
A0 and **A1** pins located on the back side of the keypad are intended to set keypad address. The keypad address is set by putting the jumper (-s) on the pins. ESIM364 system allows to connect up to 4 EKB2 keypads - each set under different address. Jumper combinations for different keypad address configuration are indicated in the table below.

Jumper position	Address
	Keypad 1
	Keypad 2
	Keypad 3
	Keypad 4

The address of each connected keypad is also indicated in *ELDES Configuration Tool* software.

32.1.1.2. Installation





32.1.1.3. Visual and Audio Indications

EKB2 can be used even in dark premises as the LCD screen and keys are illuminated continuously. The illumination level lowers down if 3 minutes after the last key-touch expires while the system is disarmed. In case of alarm, the keypad illumination level is boosted and stays in this state until the system is disarmed.

The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration, one long beep – for invalid configuration. In addition, the buzzer emits short beeps in case of alarm and exit/entry delay countdown.

32.1.1.4. EKB2 Zone and Tamper

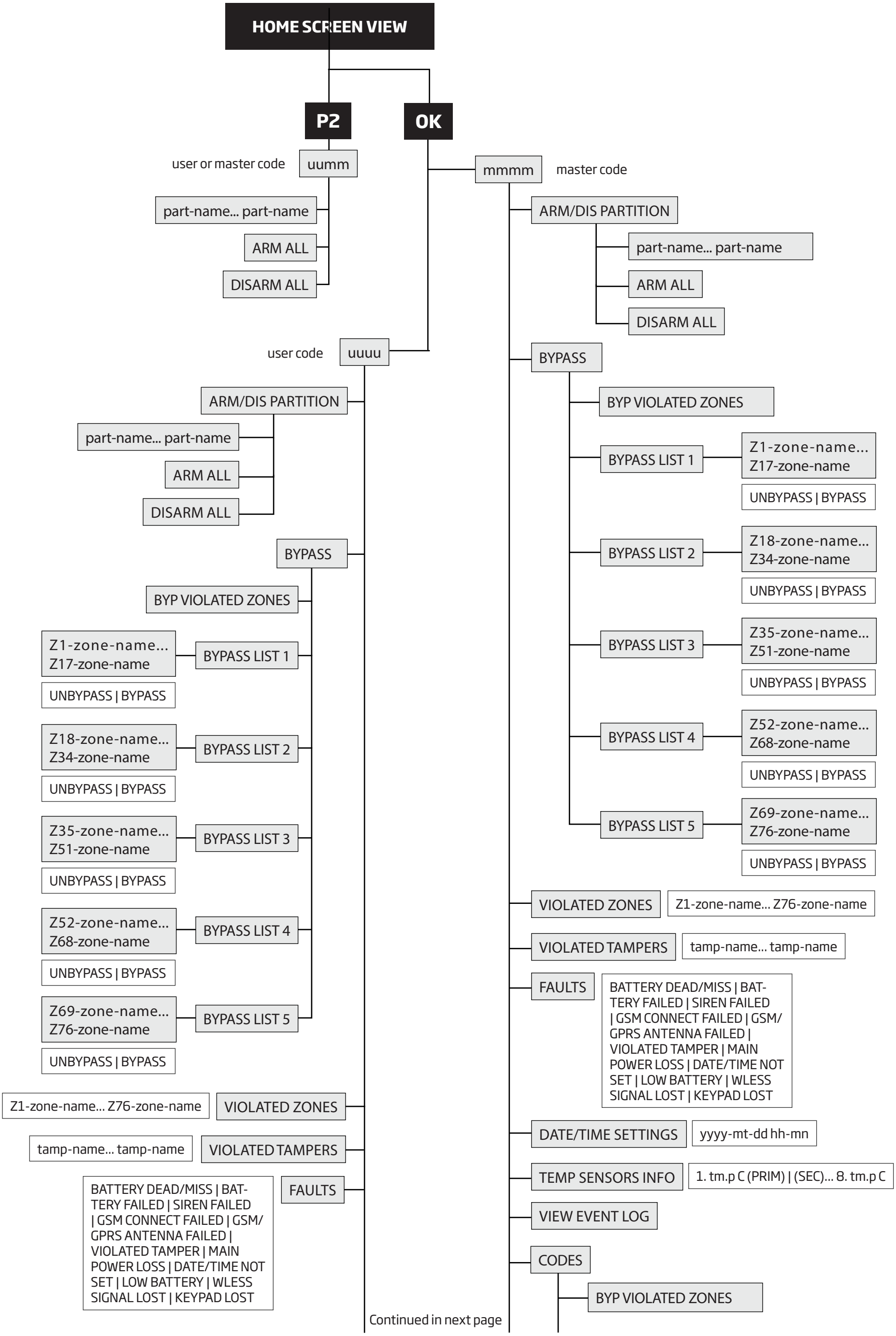
Keypad EKB2 has one wired zone Z1 and one tamper button. By default, the keypad zone Z1 is disabled. The keypad zone can be enabled by SMS, EKB2 keypad, EKB3 keypad, EKB3W keypad and *ELDES Configuration Tool* software (see **14.9. Disabling and Enabling Zones**). When Z1 is enabled, it operates like any other system zone, therefore a sensor can be connected to it. In addition, Z1 and COM terminals must be connected with resistor of 5,6kΩ nominal.

The tamper button is intended for monitoring the enclosure status of EKB2, therefore the system causes alarm if the enclosure is illegally opened. Keypad zone Z1 must be enabled and resistor connected even if the tamper button alone is required.

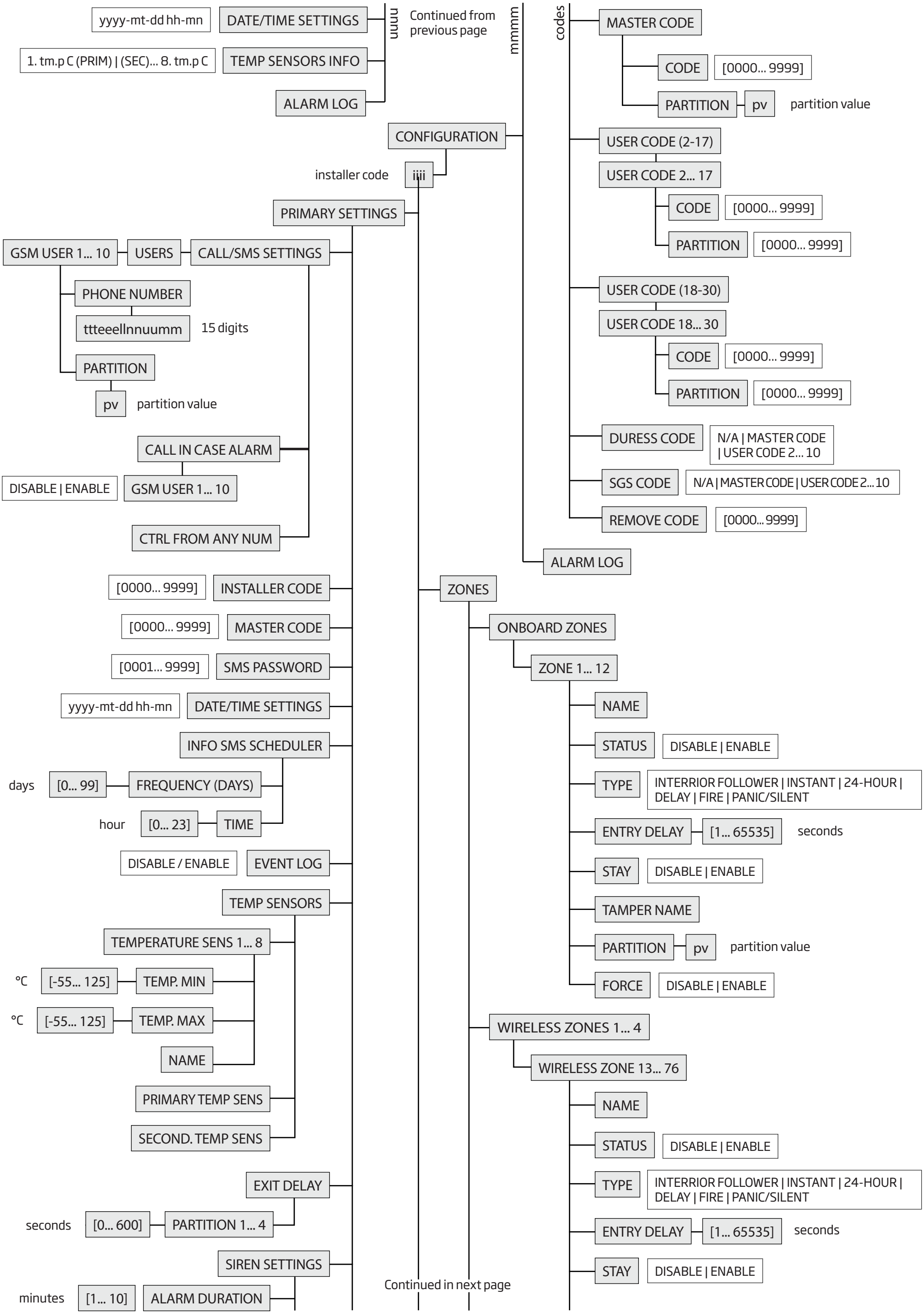
32.1.1.5. Icons and Messages

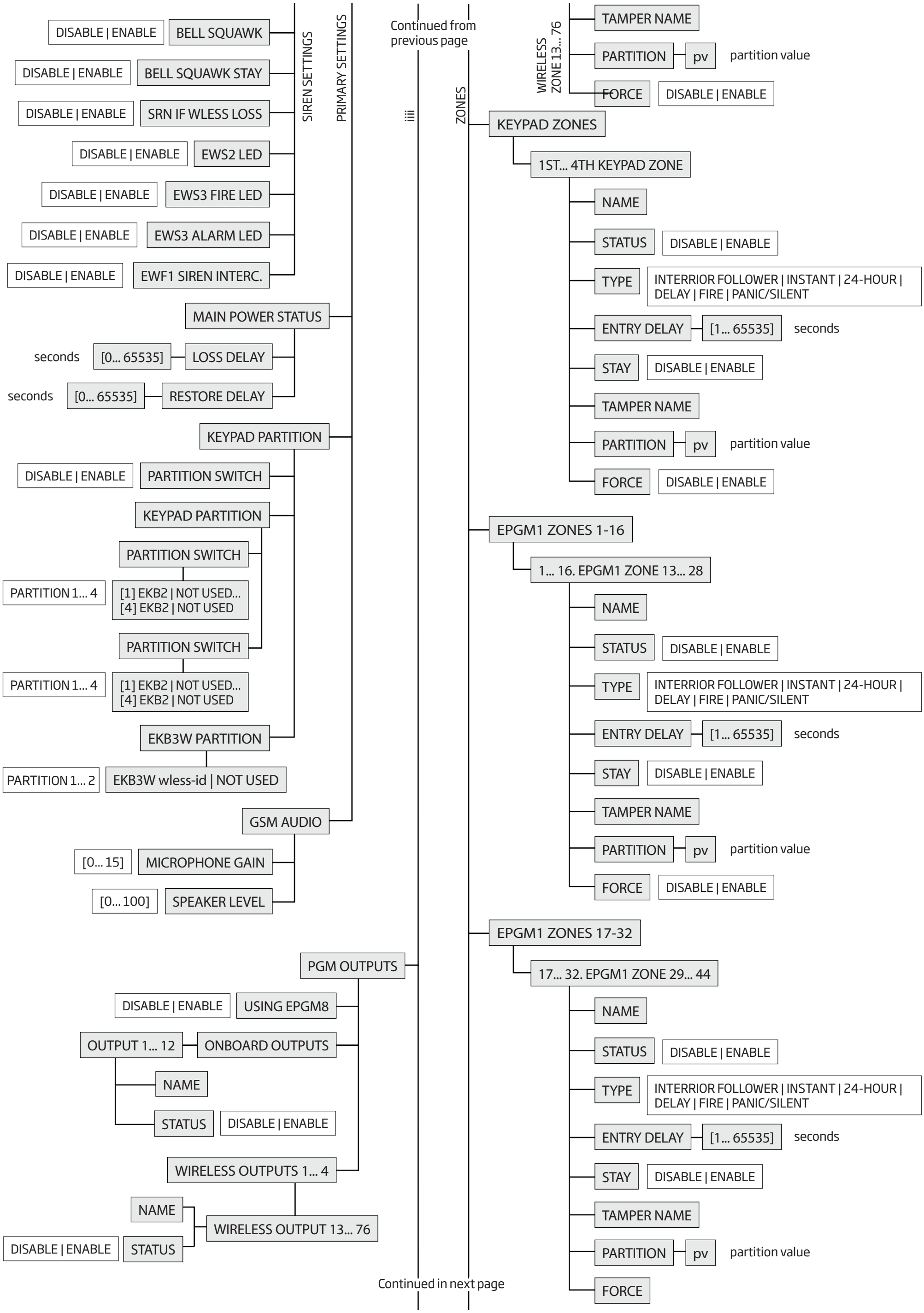
Icon / Message	Description
🔒 (by default - disabled)	Partition is armed and menu is locked
🔓 (by default - disabled)	Partition is disarmed and menu is unlocked
🛠	Configuration mode activated
! ! !	Zone or tamper alarm in partition
✓	Partition is ready to be armed.
X	Partition is not ready to be armed – one or more zones / tampers violated.
🔧!	One or more system faults present
↷	One or more violated zones bypassed
🏠	One or more partitions STAY-armed
🔥	One or more Fire-type zones violated
🔊	Alarms in alarm log present
SERVICE MODE	Service mode activated

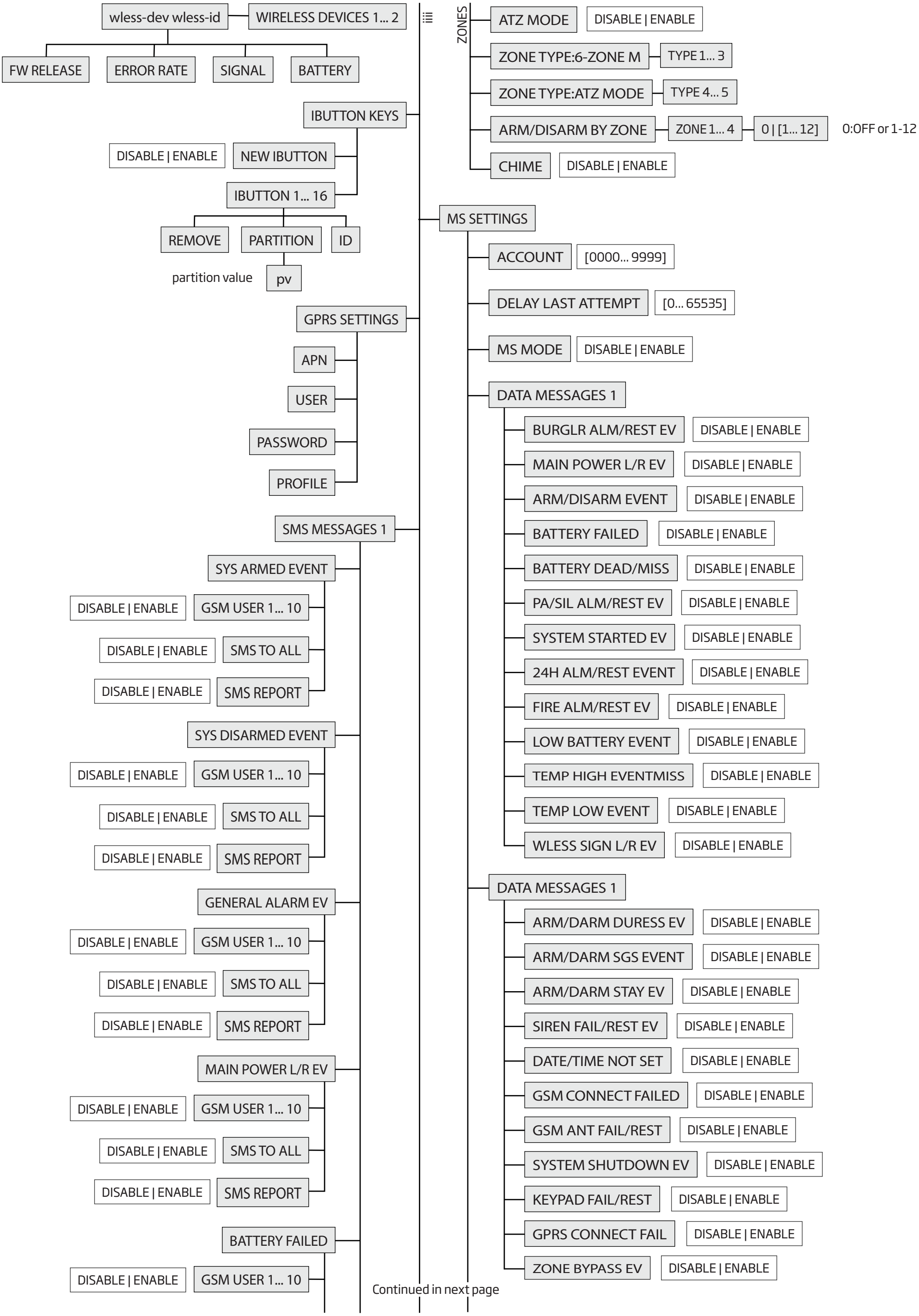
32.1.1.6. Menu Tree



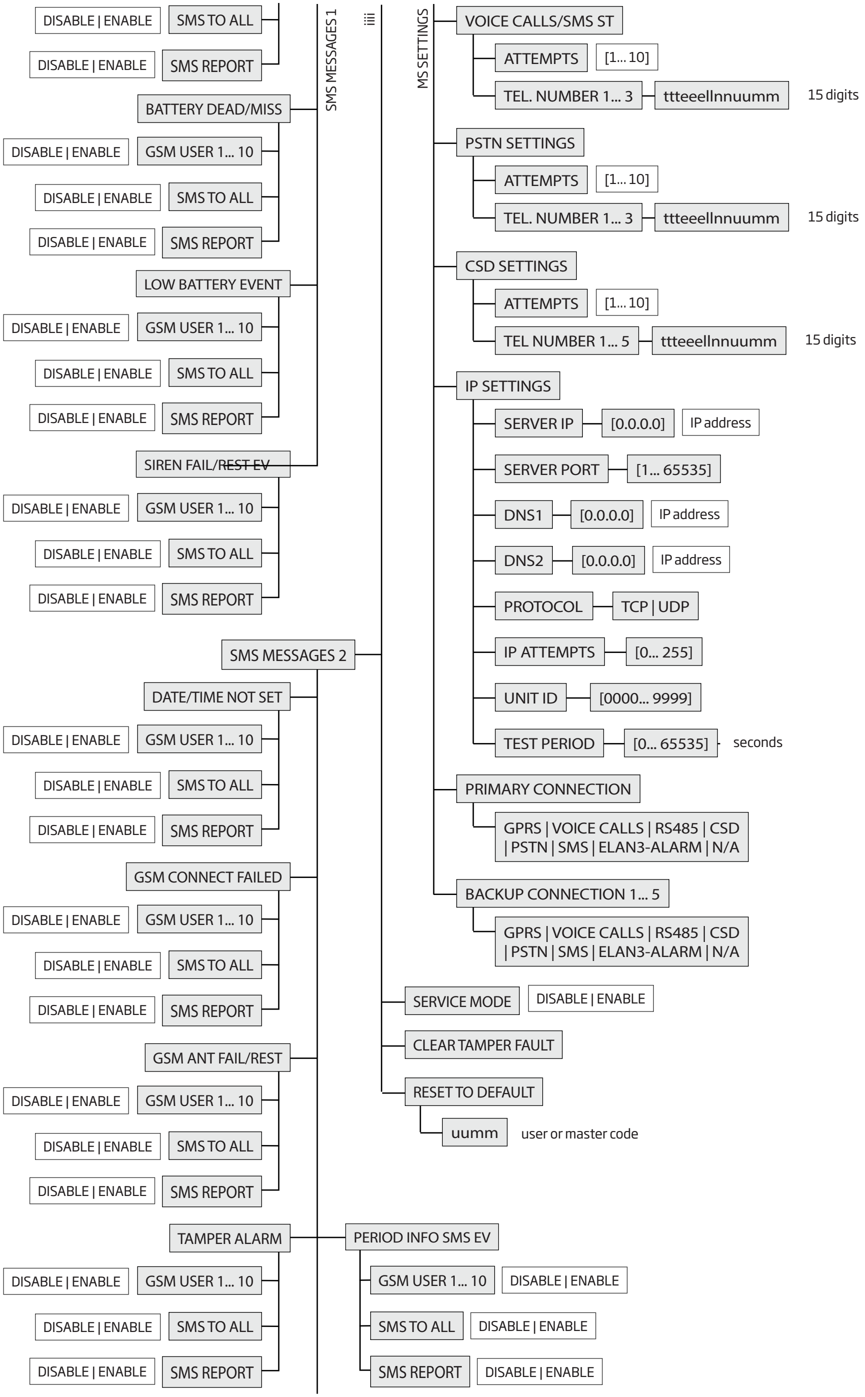
Continued in next page


yyyy-mt-dd hh-mn
DATE/TIME SETTINGS
nnnn
Continued from previous page
1. tm.p C (PRIM) | (SEC)... 8. tm.p C
TEMP SENSORS INFO
ALARM LOG
mmmm
codes
MASTER CODE
CODE
[0000... 9999]
PARTITION
pv
partition value
CONFIGURATION
installer code
iiii
USER CODE (2-17)
USER CODE 2... 17
CODE
[0000... 9999]
PRIMARY SETTINGS
PARTITION
[0000... 9999]
GSM USER 1... 10
USERS
CALL/SMS SETTINGS
PHONE NUMBER
ttteeellnnuumm
15 digits
USER CODE (18-30)
USER CODE 18... 30
CODE
[0000... 9999]
PARTITION
PARTITION
[0000... 9999]
pv
partition value
DURESS CODE
N/A | MASTER CODE | USER CODE 2... 10
CALL IN CASE ALARM
DISABLE | ENABLE
GSM USER 1... 10
SGS CODE
N/A | MASTER CODE | USER CODE 2...10
REMOVE CODE
[0000... 9999]
CTRL FROM ANY NUM
ALARM LOG
[0000... 9999]
INSTALLER CODE
ZONES
[0000... 9999]
MASTER CODE
ONBOARD ZONES
[0001... 9999]
SMS PASSWORD
ZONE 1... 12
yyyy-mt-dd hh-mn
DATE/TIME SETTINGS
NAME
INFO SMS SCHEDULER
STATUS
DISABLE | ENABLE
days
[0... 99]
FREQUENCY (DAYS)
TYPE
INTERRIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT
hour
[0... 23]
TIME
ENTRY DELAY
[1... 65535]
seconds
DISABLE / ENABLE
EVENT LOG
STAY
DISABLE | ENABLE
TEMP SENSORS
TAMPER NAME
TEMPERATURE SENS 1... 8
PARTITION
pv
partition value
°C
[-55... 125]
TEMP. MIN
FORCE
DISABLE | ENABLE
°C
[-55... 125]
TEMP. MAX
WIRELESS ZONES 1... 4
NAME
WIRELESS ZONE 13... 76
PRIMARY TEMP SENS
NAME
SECOND. TEMP SENS
STATUS
DISABLE | ENABLE
EXIT DELAY
TYPE
INTERRIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT
seconds
[0... 600]
PARTITION 1... 4
ENTRY DELAY
[1... 65535]
seconds
SIREN SETTINGS
STAY
DISABLE | ENABLE
Continued in next page
minutes
[1... 10]
ALARM DURATION

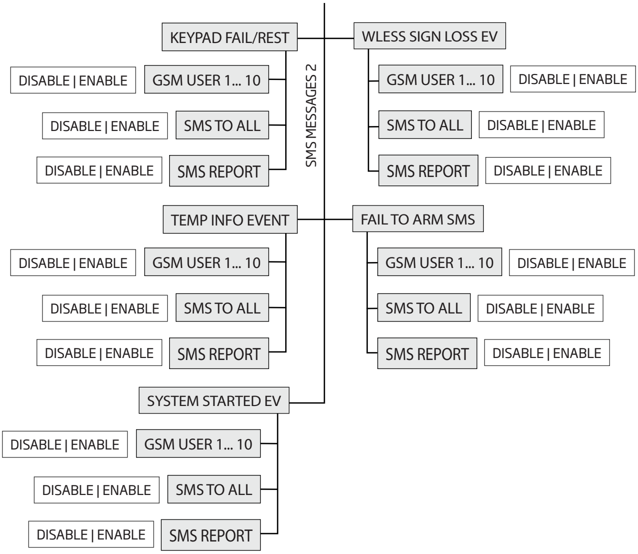

PRIMARY SETTINGS
SIREN SETTINGS
BELL SQUAWK
DISABLE | ENABLE
BELL SQUAWK STAY
DISABLE | ENABLE
SRN IF WLESS LOSS
DISABLE | ENABLE
EWS2 LED
DISABLE | ENABLE
EWS3 FIRE LED
DISABLE | ENABLE
EWS3 ALARM LED
DISABLE | ENABLE
EWF1 SIREN INTERC.
DISABLE | ENABLE
MAIN POWER STATUS
LOSS DELAY
[0... 65535]
seconds
RESTORE DELAY
[0... 65535]
seconds
KEYPAD PARTITION
PARTITION SWITCH
DISABLE | ENABLE
KEYPAD PARTITION
PARTITION SWITCH
[1] EKB2 | NOT USED...
[4] EKB2 | NOT USED
PARTITION 1... 4
PARTITION SWITCH
[1] EKB2 | NOT USED...
[4] EKB2 | NOT USED
PARTITION 1... 4
EKB3W PARTITION
EKB3W wless-id | NOT USED
PARTITION 1... 2
GSM AUDIO
MICROPHONE GAIN
[0... 15]
SPEAKER LEVEL
[0... 100]
Continued from previous page
⁞
PGM OUTPUTS
USING EPGM8
DISABLE | ENABLE
ONBOARD OUTPUTS
OUTPUT 1... 12
NAME
STATUS
DISABLE | ENABLE
WIRELESS OUTPUTS 1... 4
WIRELESS OUTPUT 13... 76
NAME
STATUS
DISABLE | ENABLE
Continued in next page
ZONES
WIRELESS ZONE 13... 76
TAMPER NAME
PARTITION
pv
partition value
FORCE
DISABLE | ENABLE
KEYPAD ZONES
1ST... 4TH KEYPAD ZONE
NAME
STATUS
DISABLE | ENABLE
TYPE
INTERRIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT
ENTRY DELAY
[1... 65535]
seconds
STAY
DISABLE | ENABLE
TAMPER NAME
PARTITION
pv
partition value
FORCE
DISABLE | ENABLE
EPGM1 ZONES 1-16
1... 16. EPGM1 ZONE 13... 28
NAME
STATUS
DISABLE | ENABLE
TYPE
INTERRIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT
ENTRY DELAY
[1... 65535]
seconds
STAY
DISABLE | ENABLE
TAMPER NAME
PARTITION
pv
partition value
FORCE
DISABLE | ENABLE
EPGM1 ZONES 17-32
17... 32. EPGM1 ZONE 29... 44
NAME
STATUS
DISABLE | ENABLE
TYPE
INTERRIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT
ENTRY DELAY
[1... 65535]
seconds
STAY
DISABLE | ENABLE
TAMPER NAME
PARTITION
pv
partition value
FORCE



Continued in next page



Continued in next page


SMS MESSAGES 2
KEYPAD FAIL/REST
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
DISABLE | ENABLE
WLESS SIGN LOSS EV
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
DISABLE | ENABLE
TEMP INFO EVENT
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
DISABLE | ENABLE
FAIL TO ARM SMS
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
DISABLE | ENABLE
SYSTEM STARTED EV
GSM USER 1... 10
DISABLE | ENABLE
SMS TO ALL
DISABLE | ENABLE
SMS REPORT
DISABLE | ENABLE

32.1.2. EKB3 - LED Keypad

EKB3 is a LED keypad intended for using with ESIM364 alarm system.

Main EKB3 features:

- Alarm system arming and disarming (see **12.4. EKB3 Keypad and User Password**).
- Arming and disarming in Stay mode (see **15. STAY MODE**).
- System parameter configuration (see **5. CONFIGURATION METHODS**).
- PGM output control (see **18.4. Turning PGM Outputs ON and OFF**).
- Visual indication by LED indicators (see **32.1.2.3. Visual and Audio Indications**).
- Audio indication by built-in buzzer (see **32.1.2.3. Visual and Audio Indications**).
- Keypad partition switch (see **23.3. Keypad Partition and Keypad Partition Switch**).

The system configuration by EKB3 keypad is performed by activating the Configuration mode (see **5. CONFIGURATION METHODS**) and entering the required parameters & values. ESIM364 system allows to connect up to 4 EKB3 keypads.

32.1.2.1. Technical Specifications

32.1.2.1.1 Electrical & Mechanical Characteristics

Power supply	12-14V ⎓ 150mA max
Maximum keypad connection cable length	100 m.
Dimensions	140x100x18mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Range of operating temperatures	-30...+55°C

32.1.2.1.2 LED Functionality

ARMED	Steady ON - alarm system is armed / exit delay in progress; flashing - Configuration mode activated
READY	Steady ON - system is ready – no violated zones and tampers
SYSTEM	Steady ON - system faults; flashing - violated high-numbered zone (-s)
BYPS	Steady ON - zone bypass mode
1-12	Steady ON - violated zone Z1-Z12

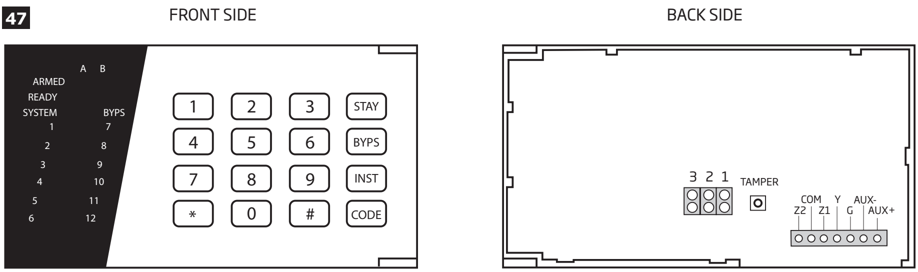
32.1.2.1.3 Keys Functionality

[BYPS]	Bypass violated zone
[CODE]	System fault list / violated high-numbered zone indication / violated tamper indication
[*]	Clear typed in characters
[#]	Confirm (enter) command
[0] ... [9]	Command typing
[1] ... [4]	Keypad partition switch / steady ON - armed partition indication / flashing - violated partition indication
[0]	Simultaneous 4-partition arming
[STAY]	Manual system arming in Stay mode
[INST]	1st character for Configuration mode activation/deactivation command

32.1.2.1.4 Connector Functionality

AUX+	Positive power supply terminal
AUX-	Negative power supply terminal
G	RS485 interface for communication (green wire)
Y	RS485 interface for communication (yellow wire)
COM	Common terminal for Z1
Z1	Security zone terminal
Z2	N/A
3, 2	Keypad address pins
1	N/A

47

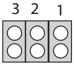
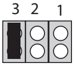
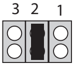
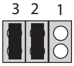

FRONT SIDE

BACK SIDE

32.1.2.1.5 Keypad Address

Pins **3** and **2** located on the back side of the keypad are intended to set keypad address. The keypad address is set by putting the jumper (-s) on the pins. ESIM364 system allows to connect up to 4 EKB3 keypads - each set under different address. Jumper combinations for different keypad address configuration are indicated in the table below.

Address Configuration

Jumper position	Address
	Keypad 1
	Keypad 2
	Keypad 3
	Keypad 4

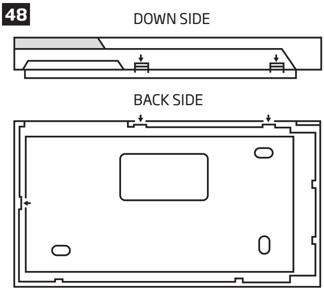
NOTE: Pins **1** are inactive.

The address of each connected keypad is also indicated in *ELDES Configuration Tool* software.

32.1.2.2. Installation

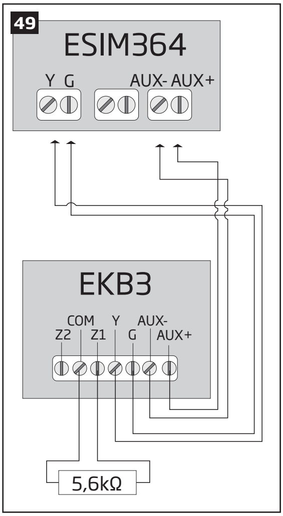
1. Detach keypad holder from EKB3 keypad . Keypad holder detach points are marked with arrows.

48


DOWN SIDE

BACK SIDE

2. Disconnect alarm system ESIM364 power supply and backup battery before connecting the wires.



3. Wire up keypad terminals to ESIM364 alarm system respectively – **AUX+** to **AUX+**, **AUX-** to **AUX-**, **Y** to **Y**, **G** to **G**. (see Fig. No. 49).
4. Connect a sensor and the resistor across Z1 and COM terminalss in accordance with zone connection Type 1 or Type 2 (see **2.3.2. Zone Connection Types**). As keypad zone Z1 is disabled by default, it can be enabled by SMS, ELDES Configuration Tool, EKB2, EKB3 and EKB3W keypad. Z2 terminal is permanently inactive. Keypad zone Z1 must be enabled and resistor connected even if the tamper button alone is required (see Fig. No. 47).

NOTE: Keypad zone connection type can differ from selected on-board zone connection type.

NOTE: ATZ mode is NOT supported by keypad zones. ATZ mode is ineffective for keypad zones when enabled.

5. Set the keypad address by combining DIP switch positions (see **32.1.2.1.5 Keypad Address**).
6. Infix the keypad into the holder (see Fig. No. 48).

ATTENTION: Before fixing the keypad into the holder please , make sure that the tamper is properly pressed (see Fig. No. 47).

7. Power up ESIM364 alarm system.
8. EKB3 keypad is ready.

For more details on multiple keypad wiring, please refer to **3.2.7. RS485.**

32.1.2.3. Visual and Audio Indications

EKB3 keys have a LED back-light, therefore it is possible to use this keypad even in dark premises. The back-light lasts for 3 minutes after the last key-stroke while the system is disarmed. In case of alarm, the keypad back-light turns ON and lasts until the system is disarmed.

The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration command, one long beep – for invalid configuration command. In addition, the buzzer emits short beeps in case of alarm and exit/entry delay countdown.

32.1.2.4. EKB3 Zone & Tamper

Keypad EKB3 has one wired zone Z1 and one tamper button. By default, the keypad zone Z1 is disabled. The keypad zone can be enabled by SMS, EKB2 keypad, EKB3 keypad, EKB3W keypad and *ELDES Configuration Tool* software (see **14.9. Disabling and Enabling Zones**). Zone Z1 is enabled, it operates like any other system zone, therefore a sensor can be connected to it. In addition, Z1 and COM terminals must be connected with resistor of 5,6kΩ nominal.

The tamper button is intended for monitoring the enclosure status of EKB3, therefore the system causes alarm if the enclosure is illegally opened. Keypad zone Z1 must be enabled and resistor connected even if the tamper button alone is required.

32.1.3. EPGM1 - Hardwired Zone & PGM Output Expansion Module

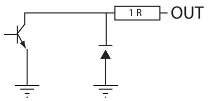
EPGM1 is a hardwired zone & PGM output expansion module intended for using with ELDES alarm systems.

Main EPGM1 features:

- Hardwired zone expansion. Each module adds 16 additional zones;
- Hardwired PGM output expansion. Each module adds 2 additional PGM outputs for electrical appliance connection;
- Up to 32 hardwired zone and up to 4 hardwired PGM output expansion.

32.1.3.1. Technical Specifications

32.1.3.1.1 Electrical & Mechanical Characteristics

Power supply	10-24V ⎓ 100mA max without auxiliary equipment.
Number of digital inputs	16
Nominal resistance	5,6kΩ
Number of PGM outputs	2
Maximum PGM output current	250 mA
EPGM1 PGM output circuit	 Open collector output. Output is pulled to COM when turned on.
Maximum commuting PGM output values	Voltage – 30V; current 250mA
AUX: auxiliary equipment power supply	13,8V ⎓ 500 mA max
Dimensions	118 x 47 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Range of operating temperatures	-20...+55°C

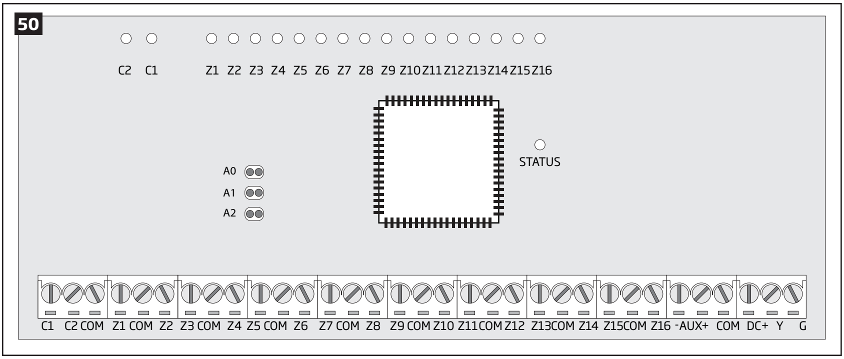
32.1.3.1.2 LED and Pin Functionality

C2, C1	PGM output C1, C2 status – on/off
Z1 - Z16	Zone Z1 - Z16 state – alarm/restore
STATUS	EPGM1 micro-controller status
A0	EPGM1 module address pins
A1	N/A
A2	N/A

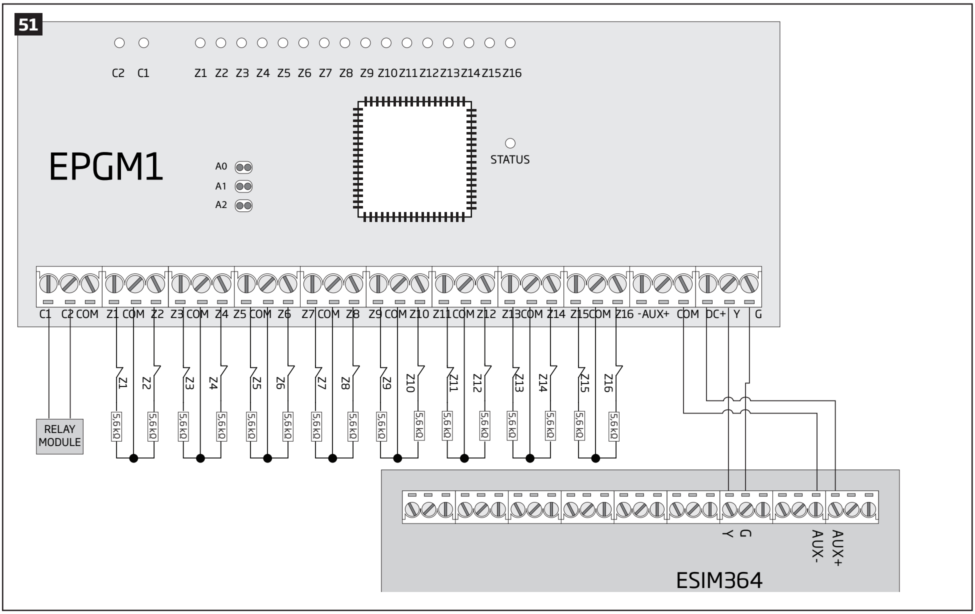
32.1.3.1.3 Connector Functionality

C1, C2	PGM output terminals
Z1 - Z16	Security zone terminals
AUX-	Negative power supply terminal for auxiliary equipment
AUX+	Positive power supply terminal for auxiliary equipment
Y	RS485 interface for communication (yellow wire)
G	RS485 interface for communication (green wire)
COM	Negative power supply terminal
DC+	Positive power supply terminal

50


C2 C1
Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8 Z9 Z10 Z11 Z12 Z13 Z14 Z15 Z16
STATUS
A0
A1
A2
C1 C2 COM Z1 COM Z2 Z3 COM Z4 Z5 COM Z6 Z7 COM Z8 Z9 COM Z10 Z11 COM Z12 Z13 COM Z14 Z15 COM Z16 -AUX+ COM DC+ Y G

51


C2 C1
Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8 Z9 Z10 Z11 Z12 Z13 Z14 Z15 Z16
EPGM1
A0
A1
A2
STATUS
C1 C2 COM Z1 COM Z2 Z3 COM Z4 Z5 COM Z6 Z7 COM Z8 Z9 COM Z10 Z11 COM Z12 Z13 COM Z14 Z15 COM Z16 -AUX+ COM DC+ Y G
RELAY MODULE
Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8 Z9 Z10 Z11 Z12 Z13 Z14 Z15 Z16
5,6kΩ
Y G
AUX- AUX+
ESIM364

32.1.3.1.4 EPGM1 Address

ESIM364 system allows to connect up to 2 EPGM1 modules - each set under different address. The module address can be set by putting or removing the jumper from the A0 pins implemented in horizontal position (see Fig. No. 50). Jumper combinations for different EPGM1 module address configuration are indicated in the table below.

Address Configuration

Jumper position	Address
●● A0	Module 1
▬ A0	Module 2

32.1.3.2. Installation

1. Disconnect ESIM364 alarm system main power supply and backup battery.
2. Connect EPGM1 **DC+** terminal to ESIM364 **AUX+** terminal, EPGM1 **COM** terminal to ESIM364 **AUX-** terminal, EPGM1 **Y** and **G** termianls must be connected to ESIM364 **Y** and **G** terminals respectively (see Fig. No. 51).
3. Connect the resistors and sensors to EPGM1 module according to the selected zone connection Type 1, Type 2 or Type 3 (see **2.3.2 Zone Connection Types**). If ATZ mode is enabled, please connect the resistors and sensors according to zone connection Type 1 or Type 2.
4. Set the EPGM1 module address by putting or removing the jumper from the A0 pins (see **32.1.3.1.4. EPGM1 Address**).
5. Power up ESIM364 system.
6. Upon successful startup indicator **STATUS** should be blinking indicating successful EPGM1 operation.
7. EPGM1 is ready for use with ESIM364 alarm system.

NOTE: ATZ mode is not supported by EPGM1 zones.

NOTE: When ATZ mode is disabled, all EPGM1 zones must be wired in accordance with zone connection type set up in the system software-wise i.e. **Type 1**, **Type 2** or **Type 3**. If ATZ mode is enabled, EPGM1 zones can be wired in accordance with **Type 1** or **Type 2** only (mixed combination of these two zone connection types is permitted), regardless of the set up zone connection type in the system.

For more details on multiple EPGM1 module wiring, please refer to **3.2.7. RS485**

32.1.4. ELAN3-ALARM - Ethernet Communicator

Main features:

- Supported Ethernet connectivity: 10/100 Mbit.
- Enables Internet access on ESIM364 via Ethernet interface.
- Automated configuration.

ELAN3-ALARM is an add-on device designed to use with ESIM364 alarm system and operate in IP-based networks. The device is an Ethernet-based communicator that enables instant Internet access allowing to perform the following:

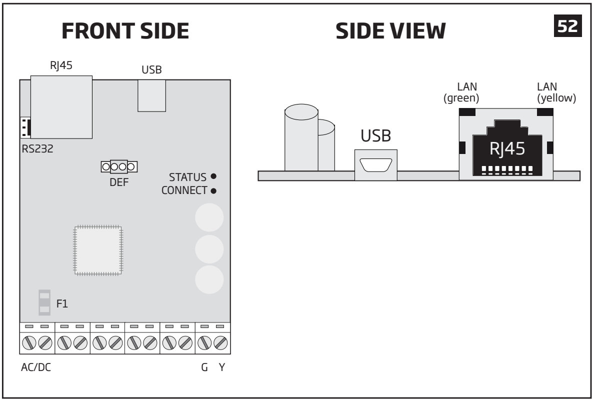
- Establish a communication between ESIM364 and EGR100 middleware, Kronos or SIA IP protocol-based monitoring station software.
- Connect ESIM364 to ELDES Smart Security platform.
- Configure ESIM364 remotely.

32.1.4.1. Technical Specifications

32.1.4.1.1 Electrical & Mechanical Characteristics

Power supply	10-24V 50Hz ~ 210mA max. / 10-24V ⎓ 210mA max.
Dimensions	70x85x57 mm
Operating temperature range	-20...+55 °C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)

32.1.4.1.2 Main Unit, LED Indicator & Connector Functionality



RJ45	10/100Base-T Ethernet port
USB	Mini USB port for firmware update
DEF	Pins for fimware update
STATUS	Red light-emitting diode indicating micro-controller status
RS485	Green light-emitting diode indicating RS485 connection status
F1	miniSMDC 0,5A fuse
AC/DC	Power supply terminals
G	RS485 interface for communication (green wire)
Y	RS485 interface for communication (yellow wire)
LAN (green)	Green light-emitting diode indicating Ethernet activity
LAN (yellow)	Yellow light-emitting diode indicating Ethernet status

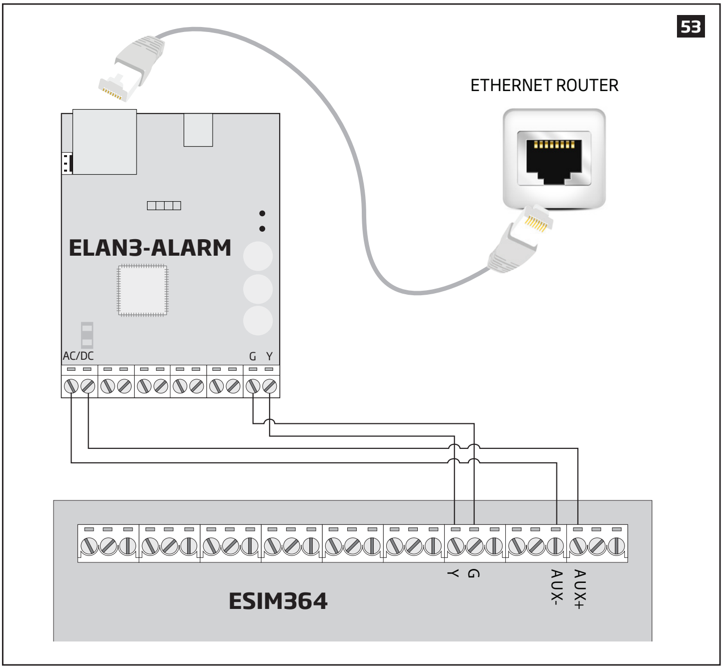
32.1.4.2. Installation

ATTENTON: The wiring is permitted to be done only while ESIM364 system is completely powered down.

1. Connect **AC/DC** terminals to ESIM364 system's **AUX+** and **AUX-** terminals. Alternatively, you can power up the device by 10-24V AC or DC power supply unit (see **32.1.5.1.1 Electrical & Mechanical Characteristics**).

2. Connect **G** and **Y** terminals to ESIM364 system's **G** and **Y** terminals respectively.

3. Connect ELAN3-ALARM to local area network router using the Ethernet cable.



4. Power up ELAN3-ALARM and wait until indicator **STATUS** starts flashing indicating successful micro-controller operation (see Fig. No. 52).
5. Indicator **LAN (green)** will flash indicating Ethernet connection activity, while indicator **LAN (yellow)** will be steady ON indicating successful Ethernet connection (see Fig. No. 52).
6. In less than 1 minute indicator **RS485** indicator will steadily light ON indicating the successfully established RS485 connection between ELAN3-ALARM device and ESIM364 system see (Fig. No. 52).
7. Once the device is up and running, it will automatically obtain a local IP address from the DHCP server, therefore manual configuration of ELAN3-ALARM is necessary only if DHCP server is not supported by your internet service provider (ISP). For more details on ELAN3-ALARM configuration, please refer to *ELDES Configuration Tool* software's HELP section.
8. Configure ESIM364 system in order to use it with ELAN3-ALARM. For more details, please refer to ESIM364 installation manual and *ELDES Configuration Tool* software's HELP section.

NOTE: Ensure that the ELAN3-ALARM device is not being blocked on the router, otherwise the device will be unable to transmit any data. To view or change the IP address of ELAN3-ALARM, please connect the device to the computer using the USB cable and *ELDES Configuration Tool* software. For more details, please refer to *ELDES Configuration Tool* software's HELP section.

32.1.4.3. Restoring Default Parameters

1. Disconnect the power supply.
2. Short circuit (connect) DEF pins.
3. Power up the device for 7 seconds.
4. Power down the device.
5. Remove short circuit from DEF pins.
6. Parameters restored to default.

32.1.4.4. Updating the Firmware via USB Cable

1. Power down the device.
2. Short-circuit (connect) the DEF pins.
3. Connect the device via USB cable to the PC.
4. Power up the device.
5. The new window must pop-up where you will find the .bin file. Otherwise open My Computer and look for Boot Disk drive.
6. Delete the .bin file found in the drive.
7. Copy the new firmware .bin file to the very same window.
8. Power down the device.
9. Unplug the USB cable.
10. Remove the short-circuit from DEF pins.
11. Power up the device.
12. Firmware updated.

32.1.5. 1-Wire Interface

1-Wire interface is used for the system to communicate with an iButton key reader and up to 8 temperature sensors. 1-Wire interface COM and DATA terminals are ground and data respectively. When connecting single or multiple temperature sensors, the +5V terminal must be used along.

For more details on 1-Wire device wiring, please refer to **32.2.1 iButton Key Reader and Buzzer**

32.1.6. iButton Key Reader and Keys

The iButton key is a chip enclosed in a stainless steel tab usually implemented in a small plastic holder. Each iButton key holds a unique identity code (ID) which is used for alarm system ESIM364 arming and disarming procedure.

Main iButton features:

- Up to 16 iButton keys per alarm system unit ESIM364;
- Communication via 1-Wire interface.

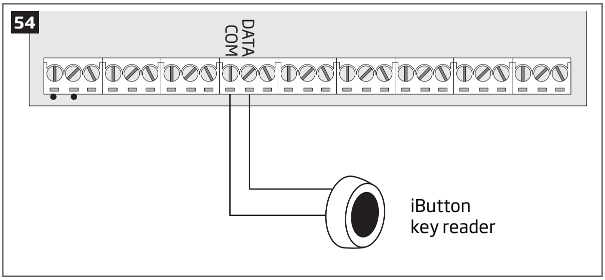
32.1.6.1. Technical Specifications

32.1.6.1.1 Electrical & Mechanical Characteristics

Supported iButton key model	Maxim/Dallas DS1990A
Communication interface	1-Wire
Maximum cable length for 1-wire communication	up to 30 meters

32.1.6.1.2 Installation

1. Disconnect ESIM364 alarm system main power supply and backup battery.
2. Connect iButton key reader contact wires to 1-Wire interface on ESIM364 alarm system: **COM** and **DATA** terminals respectively.



3. Power up ESIM364 alarm system.
4 iButton® key reader is ready for use with ESIM364 alarm system.

For more details on iButton key management, please refer to **11. iBUTTON KEYS**.

32.2. Modules Interface

32.2.1. EPGM8 - Hardwired PGM Output Expansion Module

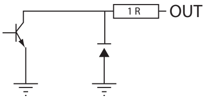
EPGM8 is a PGM output expansion module intended for using with alarm system ESIM364. This module allows to connect up to additional 8 electrical appliances.

Main EPGM8 features:

- PGM output expansion adding 8 additional PGM outputs;
- Compatible with ESIM364 alarm system

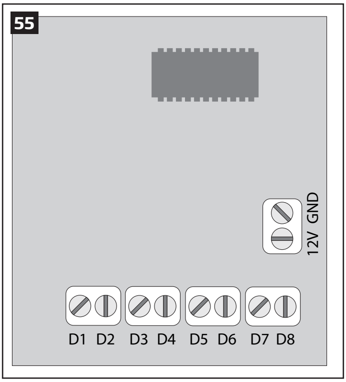
32.2.1.1. Technical Specifications

32.2.1.1.1 Electrical & Mechanical Characteristics

Power supply	10-24V ⎓ 100mA max
Number of PGM outputs	8
EPGM8 PGM output circuit	 Open collector output. Output is pulled to COM when turned on.
Maximum commuting PGM output values	Voltage – 30V; current 500mA
Dimensions	40 x 55 x 15 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Range of operating temperatures	-20...+55°C

32.2.1.1.2 Connector Functionality

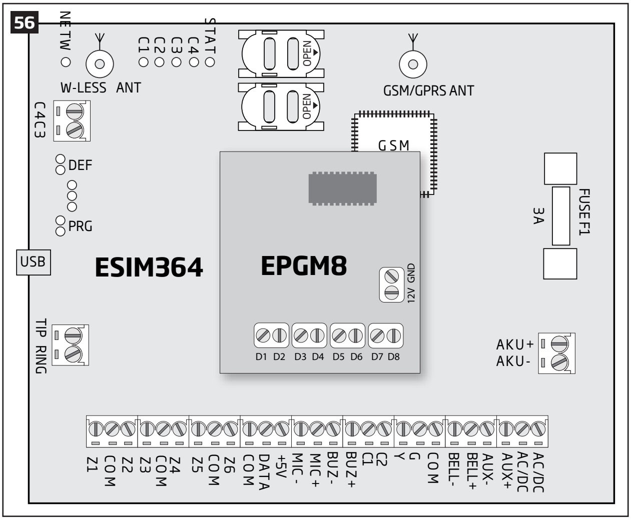
D1 - D8	PGM output terminals
12V	Positive power supply terminal
GND	Negative power supply terminal



32.2.1.2. Installation

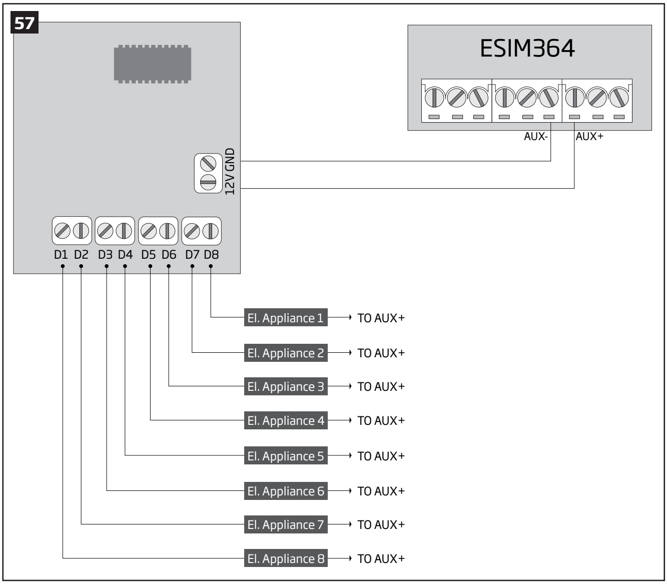
1. Disconnect ESIM364 alarm system main power supply and backup battery.
2. Insert EPGM8 pins into appropriate ESIM364 alarm system slots (see Fig. No. 54)

56



3. Connect EPGM8 **12V** positive power supply terminal with ESIM364 alarm system **AUX+** terminal and EPGM8 **GND** terminal with ESIM364 alarm system **AUX-** terminal. (see Fig. No. 55).
4. Connect the electrical appliances to **D1** – **D8** PGM outputs. (see Fig. No. 55).

57



5. Power up ESIM364 alarm system.
6. Enable EPGM8 mode using EKB2, EKB3, EKB3W keypads or *ELDES Configuration Tool* software. For more details, please refer to software's HELP section or **18.2.1. EPGM8 Mode**.
7. EPGM8 is ready for use with ESIM364 alarm system.

32.2.2. EA1 - Audio Output Module

EA1 audio output module enables a duplex audio connection for ESIM364 alarm system.

Main EA1 features:

- Two-way voice conversation during a phone call;
- Possibility to connect headphones or desktop speakers.

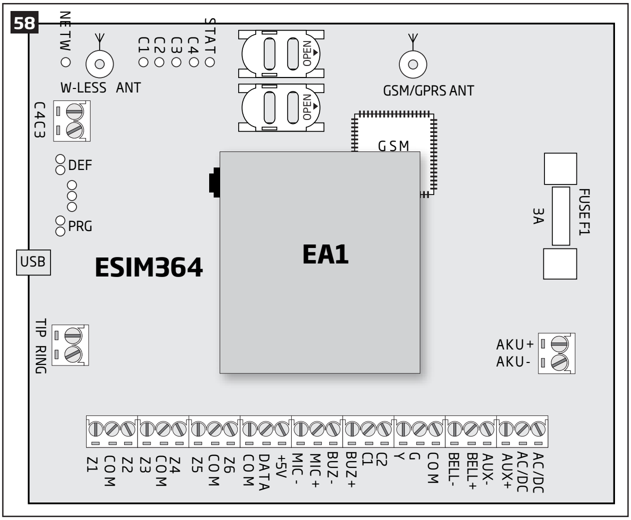
32.2.2.1. Technical Specifications

- 3,5 mm female jack
- Dimensions: 35 x 33 x 12 mm

32.2.2.2. Installation

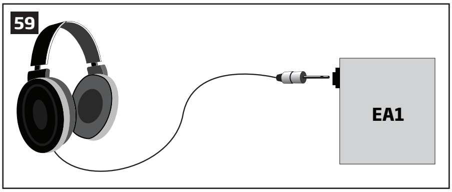
1. Disconnect ESIM364 alarm system main power supply and backup battery.
2. Insert EA1 pins into appropriate ESIM364 alarm system slots.

58



3. Connect headphones or desktop speakers to EA1 3,5 mm female jack.

59



4. Power up ESIM364 alarm system.
5. EA1 is ready for use with ESIM364 alarm system.

32.2.3. EA2 - Audio Output Module with Amplifier

EA2 audio output module enables a duplex audio connection for ESIM364 alarm system.

Main EA2 features:

- Two-way voice conversation during a phone call;
- Possibility to connect a speaker.

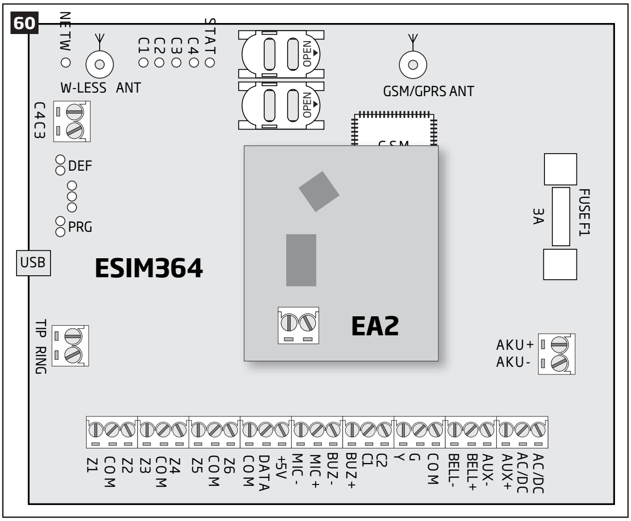
32.2.3.1. Technical Specifications

- 1W 8Ω audio amplifier
- Dimensions: 41 x 40 x 24 mm

32.2.3.2. Installation

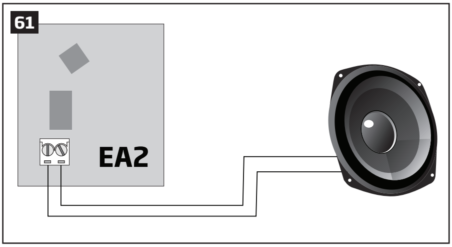
1. Disconnect ESIM364 alarm system main power supply and backup battery.
2. Insert EA2 pins into appropriate ESIM364 alarm system slots.

60



3. Connect a speaker to EA2 **Speaker** terminals.

61



4. Power up ESIM364 alarm system.
5. EA2 is ready for use with ESIM364 alarm system.

33. ELDES WIRELESS DEVICES

33.1. EKB3W - Wireless LED Keypad

EKB3W is a wireless LED keypad intended to use with ELDES alarm systems.

Main EKB3W features:

- Alarm system arming and disarming (see **12.5. EKB3W Keypad and User Password**).
- Arming and disarming in Stay mode (see **15. STAY MODE**).
- System parameter configuration (see **5. CONFIGURATION METHODS**).
- PGM output control (see **18.4. Turning PGM Outputs ON and OFF**).
- Visual indication by LED indicators (see **33.1.5. Visual and Audio Indications**).
- Audio indication by built-in buzzer (see **33.1.5. Visual and Audio Indications**).
- Keypad partition switch (see **23.3. Keypad Partition and Keypad Partition Switch**).

The system configuration by EKB3W keypad is performed by activating the Configuration mode (see **5. CONFIGURATION METHODS**) and entering the required parameters & values. ESIM364 system allows to connect up to 4 EKB3W keypads.

33.1.1. Technical Specifications

33.1.1.1. Electrical & Mechanical Characteristics

Battery type	1,5V Alkaline AAA type
Number of batteries	3
Battery operation time	~12 months*
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Range of operating temperatures	-30...+55°C
Dimensions	140 x 100 x 18 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless

* The operation time depends on different conditions and may vary.

33.1.1.2. LED Functionality

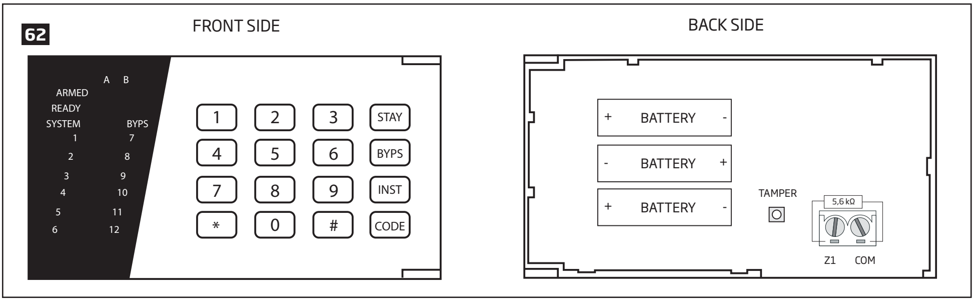
ARMED	Steady ON - alarm system is armed / exit delay in progress; flashing - Configuration mode activated
READY	Steady ON - system is ready – no violated zones and tampers
SYSTEM	Steady ON - system faults; flashing - violated high-numbered zone (-s)
BYPS	Steady ON - zone bypass mode
1-12	Steady ON - violated zone Z1-Z12

33.1.1.3. Keys Functionality

[BYPS]	Bypass violated zone
[CODE]	System fault list / violated high-numbered zone indication / violated tamper indication
[*]	Clear typed in characters
[#]	Confirm (enter) command
[0] ... [9]	Command typing
[1]... [2]	Keypad partition switch
[0]	Simultaneous 4-partition arming
[STAY]	Manual system arming in Stay mode
[INST]	1st character for Configuration mode activation/deactivation command

33.1.1.4. Main Unit & Connector Functionality

62

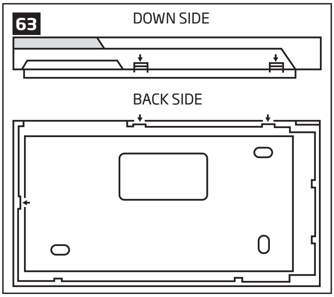


TAMPER	Tamper-button for EKB3W enclosure status monitoring	COM	Common contact
+ / -	Battery slots	Z1	Security zone terminal

33.1.2. Installation

1. Detach keypad holder from EKB3W front side . Keypad holder detach points are marked with arrows.

63



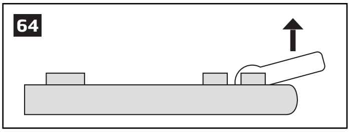
2. Fix the keypad holder on the wall using the screws.
3. Connect a sensor and the resistor across **Z1** and **COM** terminalss in accordance with zone connection Type 1 or Type 2 (see **2.3.2. Zone Connection Types**). As keypad zone **Z1** is disabled by default, it can be enabled by SMS, *ELDES Configuration Tool*, EKB2, EKB3 and EKB3W keypad. Keypad zone **Z1** must be enabled and resistor connected even if the tamper button alone is required (see Fig. No. 62).

NOTE: Keypad zone connection type can differ from selected on-board zone connection type.

NOTE: ATZ mode is NOT supported by keypad zones. ATZ mode is ineffective for keypad zones when enabled.

4. Remove the plastic tab inserted between one of the battery terminals and battery slots.

64



ATTENTION: Before fixing the keypad into the holder please , make sure that the tamper is properly pressed (see Fig. No. 62)..

5. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool software*. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EKB3W closer to alarm system device and bind it again.
7. Upon the successful binding process, the built-in mini buzzer of EKB3W device provides 3 short beeps and the system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EKB3W closer to alarm system device and bind anew.
8. EKB3W keypad is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.1.6. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM364 system can be 0,5 meters.

33.1.3. EKB3W Zone & Tamper

Upon successful EKB3W wireless LED keypad contact binding process, the system adds 1 wireless Instant zone intended for wired sensor connection. By default, the keypad zone Z1 is disabled. The keypad zone can be enabled by SMS, EKB2 keypad, EKB3 keypad, EKB3W keypad and *ELDES Configuration Tool*. software (see **14.9. Disabling and Enabling Zones**). When Z1 is enabled, it operates like any other system zone, therefore a sensor can be connected to it. In addition, Z1 and COM terminals must be connected with resistor of 5,6kΩ nominal.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EKB3W:

- **By tamper button.** EKB3W has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EKB3W is illegally opened, the tamper button becomes unpressed (see Fig. No. 62). This action is followed by alarm which is sent by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EKB3W and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS message contains the wireless device model, wireless ID code and tamper number.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

33.1.4. Battery Replacement

1. Open EKB3W enclosure.
2. Remove all 3 old batteries from the battery slots.
3. Postition the 3 new 1,5V alkaline AAA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EKB3W.
4. Insert the batteries into the battery slots.
5. Batteries replaced.

For more details, please refer to **33.1.2. Installation**.

ATTENTION: Only 1,5V Alkaline AAA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

33.1.5. Visual and Audio Indications

EKB3W keys have a LED back-light, which will be activated once any key is pressed. Due to battery power saving reasons, the back-light and LED light last for 10 seconds after the last key-stroke.

The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration command, one long beep – for invalid configuration command. The buzzer emits short beeps during exit delay. Due to battery saving reasons the buzzer will beep during entry delay and in case of alarm only if the violated zone is of the associated EKB3W keypad.

NOTE: The keypad will not activate any LED indicators, nor the back-light if not bound to the system.

For more details, please refer to **33.1.7. Wireless Communication, Sleep Mode and Back-light Timeout**

33.1.6. Restoring Default Parameters

1. Remove one battery from EKB3W.
2. Press and hold the [*] key.
3. Insert the battery back to EKB3W.
4. Hold the [*] key until LED **READY** starts flashing.
5. Wait until LED **READY** turns off and LED **ARMED** starts flashing.
6. Release the [*] key.
7. Parameters reset to default.

33.1.7. Wireless Communication, Sleep Mode and Back-light Timeout

Once the wireless device is bound, it will attempt to exchange data with ESIM364 system. The communication process follows this pattern:

1. Due to battery power saving reasons, most of the time EKB3W keypad operates in sleep mode and periodically wakes up (by default - every 60 seconds) to transmit the supervision signal, identified as Test Time, to the ESIM364 system. However, when the keypad wakes up, it will NOT activate its buzzer and/or the LED indicators.

2. When any EKB3W key is pressed, the keypad LED indicators and the back-light will activate for a set up period of time (by default - 10 seconds), identified as Back-light Timeout. During the Back-light Timeout, the Test Time will automatically switch to 2 seconds period allowing to indicate system alarms, faults and arm/disarm process on the EKB3W keypad if it is assigned to the same partition as the one that is violated or being armed/disarmed (see **23. PARTITIONS)**.

3. The Back-light timeout will expire after 10 seconds (by default) of EKB3W idling. When the Back-light Timeout expires, the keypad will light OFF the LED indicators and the back-light and return to sleep mode. Meanwhile:

   a) if a zone or tamper, which is of the associated EKB3W keypad, is violated, EKB3W will instantly wake up and initiate the Back-light Timeout. Meanwhile the keypad buzzer will emit short beeps and the LED indicators will light ON indicating the violated zone or tamper number.

   b) if a zone or tamper, which is not of the associated EKB3W keypad, is violated, EKB3W keypad will NOT wake up and will NOT initiate the Back-light Timeout as well as the buzzer will NOT emit short beeps and the LED indicators will NOT light ON.

To set a different Back-light Timeout value, please refer to the following configuration method:

Set Back-light Timeout

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details and how to set a different Test Time value, please refer to **19. WIRELESS DEVICES.**

NOTE: Even if Back-light Timeout has expired, the character will be considered as type in once the appropriate EKB3W key is pressed.

33.2. EW1 - Wireless Zone & PGM Output Expansion Module

Main EW1 features:

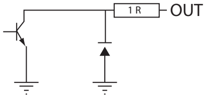
- 2 zones for wired sensor connection;
- 2 PGM outputs for electrical appliance connection;
- Powered by external power supply.

Wireless expansion module EW1 is a wireless device with 2 zones and 2 PGM outputs. This expansion module connects to ELDES wireless alarm systems and enables wireless access for to 2 wired devices such as movement PIR sensors, magnetic door contacts etc. In addition it allows to connect and control up to 2 appliances, i.e. lighting, heating etc. After the wiring process to EW1 it is necessary to bind EW1 to the alarm system by sending a corresponding command via SMS text message or using software *ELDES Configuration Tool.*

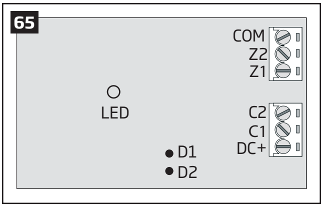
It is possible to connect up to 32 EW1 devices to ESIM364 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

33.2.1. Technical Specifications

33.2.1.1. Electrical & Mechanical Characteristics

Power supply	7-15V ⎓ 20mA max
Number of zones	2
Zone connection type	Normally closed (NC)
Number of PGM outputs	2
Maximum commuting PGM output values	Voltage – 30V; current 500mA
EW1 PGM output circuit	 Open collector output. Output is pulled to COM when turned on.
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Range of operating temperatures	-20...+55°C
Dimensions	38x60x12mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless

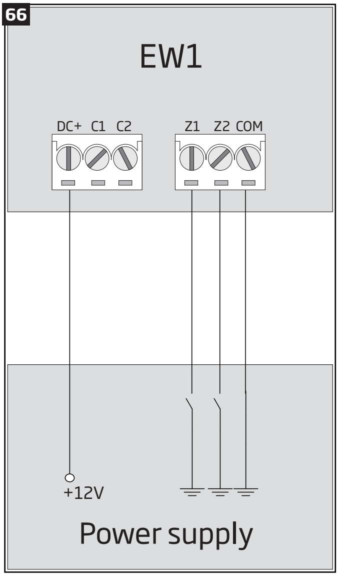
65



33.2.1.2. Connector & LED Functionality

COM	Common terminal for power supply, zones
Z2, Z1	Security zone terminals
C2, C1	PGM output terminals
DC+	Positive power supply terminal
D1, D2	Pins for restoring default parameters
LED	EW1 status

66



33.2.2. Installation

1. Disconnect ESIM364 alarm system main power supply and backup battery.
2. Wire up EW1 as indicated in Fig. No. 66.
3. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
4. T he system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EW1 closer to ESIM364 alarm system device and bind it again.
5. EW1 module is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.2.4 Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM364 system can be 0,5 meters.

33.2.3. EW1 Zones, PGM Outputs & Tamper

Upon successful EW1 module binding process, the system adds 2 wireless Instant zones intended for wired sensor connection and 2 wireless PGM outputs intended for electrical appliance connection and control.

The wireless connection loss between EW1 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS message contains the wireless device model, wireless ID code and tamper number.

ATTENTION: The tamper will not operate if both wireless zones are disabled.

33.2.4. Restoring Default Parameters

1. Disconnect EW1 power supply.
2. Short circuit (connect) pins D1 and D2.
3. Power up EW1 and wait until LED provides several short flashes.
4. Disconnect power supply.
5. Remove short-circuit from D1 and D2 pins.
6. Power up EW1.
7. Parameters restored to default.

33.3. EWP1 – Wireless Motion Detector

Main EWP1 features:

- Violated zone detection by built-in PIR movement sensor.

EWP1 is a wireless device with built-in PIR movement sensor and operates with ELDES wireless alarm systems. The user only needs to switch on the EWP1 sensor and bind it to ESIM364 alarm system by sending a corresponding command via SMS text message or using software *ELDES Configuration Tool*. User can also monitor temperature of the surrounding areas in real-time as EWP1 has a built-in temperature sensor. It is possible to connect up to 32 EWP1 devices to ESIM364 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

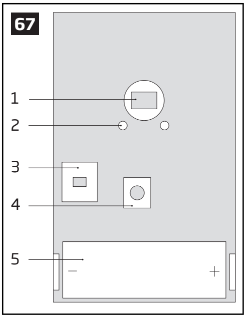
33.3.1. Technical Specifications

33.3.1.1. Electrical & Mechanical Characteristics

Battery type	ER14505 AA Lithium Thionyl Chloride
Battery voltage; capacity	3,6 V; 2,4 Ah
Battery operation time	~18 months*
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Range of operating temperatures	-10 ... +55°C
Dimensions	104x60x33mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Detection coverage angle	90°
Maximum detection distance	10 meters
Compatible with alarm systems	ELDES Wireless
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas

* The operation time depends on different conditions and may vary.

67



1 Motion detector

2 LED indicators informing about status of PIR sensor EWP1

3 TAMPER button automatically identifies when the box of sensor EWP1 is open or closed

4 RESET button for reseting system parameters

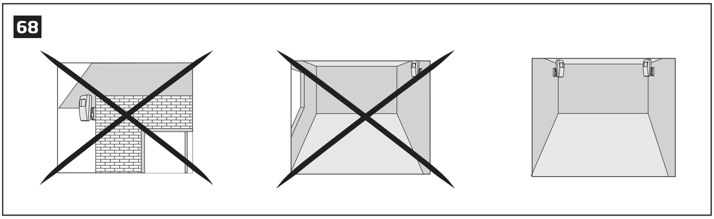
5 ER14505 3,6 V Lithium Thionyl Chloride battery

33.3.2. Installation

1. Choose the place where intrusion into the premises is the most probable and install the device. To avoid false triggers of the system do not install it in the following places:

- directing the lens to direct sunlight, for example, to the window of the premises;
- where there is a risk of sudden temperature alteration, for example, near a fireplace or heating system;
- where there is an enlarged possibility of dust or air flow;
- behind the curtain or some other cover blocking the detected zone.

68



2. Fix EWP1 sensors mounting holder with two screws to the wall and attach the sensor.
3. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
4. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWP1 closer to alarm system device and bind it again.
5. EWP1 is ready to use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.3.5. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM364 system can be 0,5 meters.

33.3.3. EWP1 Zone & Tamper

Upon successful EWP1 sensor binding process, the system adds 1 wireless Instant zone intended for movement detection. By, default, the alarm is caused instantly if any movement is detected in coverage area of the sensor (when system is armed).

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWP1 sensor:

- **By tamper button.** EWP1 has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EWP1 is illegally opened, the tamper button becomes unpressed (see Fig. No. 67). This action is followed by alarm which is sent by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWP1 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS message contains the wireless device model, wireless ID code and tamper number.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

33.3.4. Battery Replacement

1. Open EWP1 enclosure.
2. Remove the old battery from the battery slot.
3. Postition the new battery according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWP1.
4. Insert the battery into the battery slot.
5. Batteries replaced.

For more details, please refer to **33.3.2. Installation.**

ATTENTION: Only ER14505 Lithium Thionyl Chlorid AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

33.3.5. Restoring Default Parameters

1. Remove any battery from EWP1.
2. Press and hold the RESET button.
3. Insert the battery back to EWP1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

33.4. EWD1 – Wireless Magnetic Door Contact

Main EWD1 features:

- Violated zone detection by magnetic contact;
- Panic button.

EWD1 is a wireless device with magnetic contact and panic button which is used to secure doors, windows or any other opening parts and it operates with ELDES wireless alarm systems. EWD1 is bind to ESIM364 alarm system by sending a corresponding command via SMS text message or using software *ELDES Configuration Tool.* When EWD1 is connected to the system, two wireless zones are added. First wireless zone is used to monitor the magnetic contacts and the second wireless zone is for managing the panic button. By default panic button zone is configured as Silent zone and in case the panic button is pressed, the system causes silent alarm (no siren is activated).

It is possible to connect up to 32 EWD1 devices to ESIM364 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

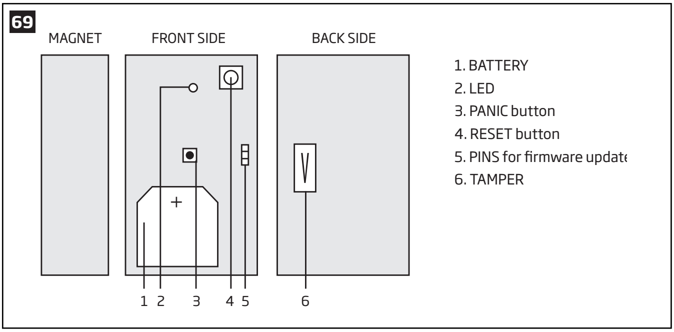
33.4.1. Technical Specifications

33.4.1.1. Electrical & Mechanical Characteristics

Battery type	CR2032 3V Lithium
Number of batteries	1
Battery operation time	15 months*
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Range of operating temperatures	-20...+55°C
Door contact dimensions	60x37x18mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Magnet dimensions	60x17x16mm
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless

* The operation time depends on different conditions and may vary.

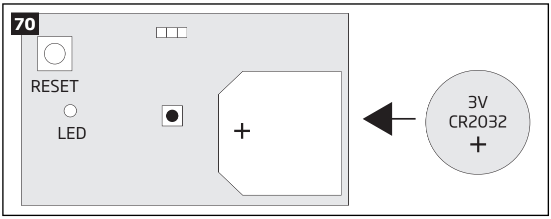
69



33.4.2. Installation

1. Open EWD1 enclosure and insert the battery.

70

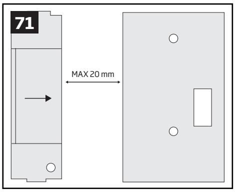


2. EWD1 consists of two parts: a magnet and a sensor. Sensor components are: a mounting part and the sensor. Magnet components are: a mounting part and the cover.

2.1 Fix the sensor mounting part with two screws on the door or window jamb.

2.2 Fix the magnet mounting part with two screws next to the sensor mounting part on door or window frame.

71



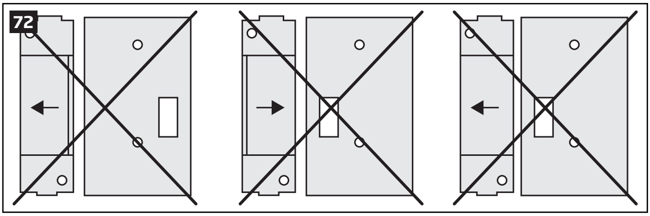
NOTE: The distance between magnet and sensor can be up to 20 mm only.

2.3 The sensor should be attached to the fixed sensors mounting part. When attaching sensor pay attention to the tamper (micro switch) - it must be pressed.

2.4 The magnet cover should be attached to the fixed magnet mounting part.

NOTE: It is not recommend to fix EWD1 in other ways than with screws, e.g. with duck tape. See Fig. No. 69 for the incorrect ways of fixing the magnetic door contact.

72



3. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.

4. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWD1

closer to alarm system device and bind it again.

5. EWD1 magnetic door contact is ready to use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.4.5. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM364 system can be 0,5 meters.

33.4.3. EWD1 Zones & Tamper

Upon successful EWD1 magnetic door contact binding process,the system adds 1 wireless Instant zone and 1 wireless Panic/Silent zone. The wireless zones are applied to the following EWD1 components respectively:

- **Magnetic contact -** by default, causing alarm if doors/windows is opened when system is armed.
- **Panic button** - by default, causing silent alarm instantly when pressed.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWD1:

- **By tamper button.** EWD1 has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EWD1 is illegally opened, the tamper button becomes unpressed (see Fig. No. 69). This action is followed by alarm which is sent by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWD1 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS message contains the wireless device model, wireless ID code and tamper number.

ATTENTION: The tamper will not operate if both wireless zones are disabled.

33.4.4. Battery Replacement

1. Open EWD1 enclosure.
2. Remove the old battery from the battery slot.
3. Postition the new battery according to the appropriate battery slot positive terminal indicated.
4. Insert the battery into the battery slot.
5. Battery replaced.

For more details, please refer to **33.4.2. Installation.**

ATTENTION: Only ER14505 Lithium Thionyl Chlorid AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

33.4.5. Restoring Default Parameters

1. Remove the battery from EWD1.
2. Press and hold the RESET button.
3. Insert the battery back to EWD1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

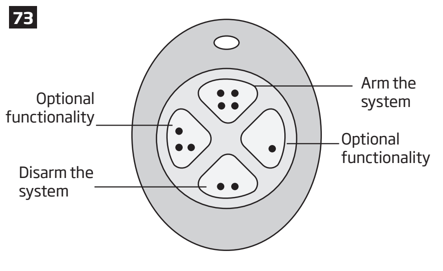
33.5. EWK1 - Wireless Keyfob

Main EWK1 features:

- Alarm system arming & disarming;
- Panic button;
- PGM output control;
- Sound indication by built-in mini buzzer.

Keyfob EWK1 – is a wireless device intended to arm and disarm ESIM364 alarm system, to open and close the gates or to control any other device connected to the alarm system. Wireless keyfob EWK1 is compatible with ELDES wireless alarm systems, therefore user can easily bind it to the alarm system using *ELDES Configuration Tool* software or sending a corresponding SMS command. EWK1 keyfob features four configurable buttons intended to operate according to individual needs. After the button is pressed, EWK1 internal buzzer's sound signal confirms a transferred command to ESIM364 alarm system via wireless connection. The status of the sent command can be checked by attempting to receive the feedback signal from the alarm system. This can be performed by pressing down the same button and holding it for 3 seconds. 3 short sound signals indicate a successfully carried out command while 1 long beep stands for failed command and feedback signal failure. By default one pair of buttons is already configured to arm and disarm the alarm system.

73



The virtual zones of ESIM364 system are intended for EWK1 button configuration. Please, refer to software's *ELDES Configuration Tool* HELP section for more details.

It is possible to connect up to 5 EWK1 devices to ESIM364 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

NOTE: The picture above reflects the default EWK1 button configuration. All keyfob buttons are configurable according to individual needs.

33.5.1. Technical Specifications

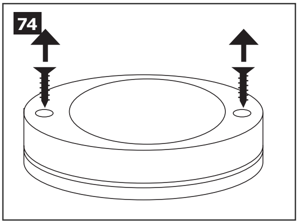
33.5.1.1. Electrical & Mechanical Characteristics

Battery type	CR2032 Lithium
Battery voltage; capacity	3V; 240 mAh
Quantity of batteries	1
Battery operation time	~18 months*
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Range of operating temperatures	-20...+55°C
Wireless keyfob dimensions	54 x 42 x 13 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless

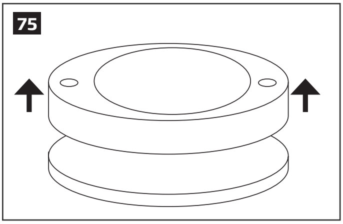
* The operation time depends on different conditions and may vary.

33.5.2. Installation

74



75

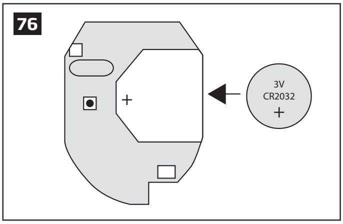


1. Unscrew the EWK1 keyfob housing.

2. Open EWK1 keyfob housing.

3. Insert CR2032 battery provided in the EWK1 package.
   Before inserting the battery, make sure that the battery's "+" sign is facing the outer side.

76



4. Close and screw up the keyfob housing.
5. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. While binding the device to the alarm system, press any EWK1 button several times.
7. EWK1 is ready to use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.5.5. Restoring Default Parameters** for more details.

33.5.3. EWK1 Zones (Panic Button)

EWK1 keyfob supports a Panic Button feature allowing to cause alarm at any time when the specified button is pressed. This feature can be configured using *ELDES Configuration Tool* software by creating a virtual zone of Panic/Silent or 24-Hour type and assigning it to Virtual Alarm option. The Panic Button feature can be set up on any button of EWK1. For more details, please refer to software's HELP section.

33.5.4. Battery Replacement

1. Open EWD1 enclosure.
2. Remove the old battery from the battery slot.
3. Postition the new battery according to the appropriate battery slot positive terminal indicated.
4. Insert the battery into the battery slot.
5. Battery replaced.

For more details, please refer to **33.5.2 Installation.**

ATTENTION: Only CR2032 3V batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

33.5.5. Restoring Default Parameters

1. Remove the battery from EWK1 keyfob.
2. Press and hold ∵ button.
3. Insert the battery back to EWK1.
4. Hold the button pressed until LED indicator provides several short flashes.
5. Release ∵ button.
6. Parameters restored to default.

33.6. EWS1 - Wireless Indoor Siren

Main EWS1 features:

- Audio alarm indication by built-in speaker.

EWS1 is a wireless device with built-in siren speaker and operates with ELDES wireless alarm systems. EWS1 has to be bind to the alarm system by sending a corresponding SMS text message or using software *ELDES Configuration Tool*. Upon successful EWS1 binding, the system adds one wireless zone and one wireless PGM output. The wireless zone is used to monitor the device (tamper - when the batteries are being removed) and the wireless PGM output is used to control the speaker. In case of alarm, the siren provides a sound alarm for one minute. The configuration of this parameter is disabled for EWS1 in order to save the battery power.

It is possible to connect up to 32 EWS1 devices to the alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

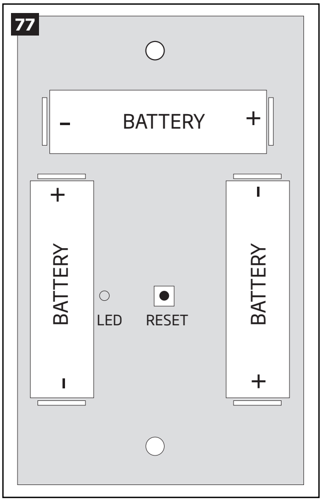
33.6.1. Technical Specifications

33.6.1.1. Electrical & Mechanical Characteristics

Battery type	1,5V Alkaline AA type
Number of batteries	3
Battery operation time	~18 months*
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Range of operating temperatures	-20...+55°C
Dimensions	123x73x36mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless
Acoustic sound level	~97 dB measured at 1 m

* The operation time depends on different conditions and may vary.

77



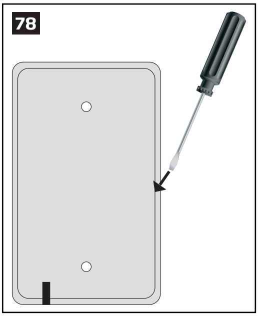
33.6.1.2. Main Unit & LED Functionality

RESET	Button for restoring default parameters
+ / -	Battery slots
LED	EWS1 status indication

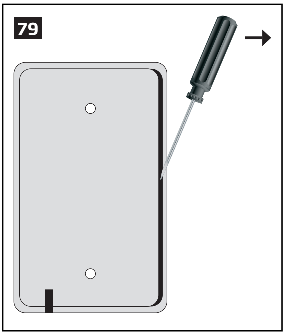
33.6.2. Installation

1. Open EWS1 enclosure.

78



79

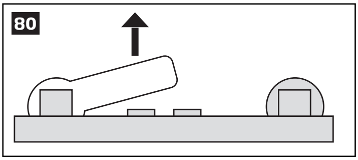


Insert a thin flat-shaped screwdriver or any tool alike into the gap located on the back of the enclosure.

Push the screwdriver down to the right carefully in order to detach the enclosure parts from each other.

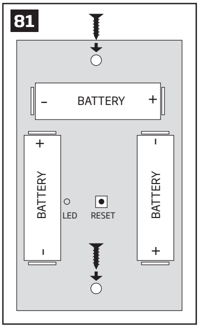
2. Once the enclosure is opened, remove the plastic tab inserted between one of the battery terminals and battery slots.

80



3. Fix the siren on the wall using the screws.

81



4. Close EWS1 enclosure. No tools are required for this action.
5. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWS1 closer to alarm system device and bind it again.
7. EWS1 siren is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.6.5. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM364 system can be 0,5 meters.

33.6.3. EWS1 Zone, PGM Output & Tamper

Upon successful EWS1 indoor siren binding process,the system adds 1 wireless Instant zone and 1 wireless Siren PGM output. The wireless zone is intended for EWS1 tamper control and the wireless PGM output is for siren control.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. The wireless connection loss between EWS1 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS message contains the wireless device model, wireless ID code and tamper number.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

ATTENTION: The siren will sound only if wireless zone of the siren is assigned to the same partition as the one that has been alarmed (see **23.1. Zone Partition**).

33.6.4. Battery Replacement

1. Open EWS1 enclosure.
2. Remove all 3 old batteries from the battery slots.
3. Postition the 3 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWS1
4. Insert the batteries into the battery slots.
5. Batteries replaced.

For more details, please refer to **33.6.2 Installation**.

ATTENTION: Only CR2032 3V batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

33.6.5. Restoring Default Parameters

1. Remove any battery from EWS1.
2. Press and hold the RESET button.
3. Insert the battery back to EWS1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

33.7. EWS2 - Wireless Outdoor Siren

Main EWS2 features:

- Audio alarm indication by built-in speaker;
- Visual alarm indication by built-in LED indicators;
- Range of operating temperature: -30...+55°C.

EWS2 is a wireless outdoor device with a built-in siren speaker, LED indicators and operates with ELDES wireless alarm systems. EWS2 has to be bind to the alarm system by sending a corresponding SMS text message or using software *ELDES Configuration Tool*. Upon successful EWS2 binding process, the system adds one wireless zone and one wireless PGM output. In case of alarm, the siren provides a sound alarm for one minute. The configuration of this parameter is disabled for EWS2 in order to save the battery power.

It is possible to connect up to 32 EWS2 devices to the alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

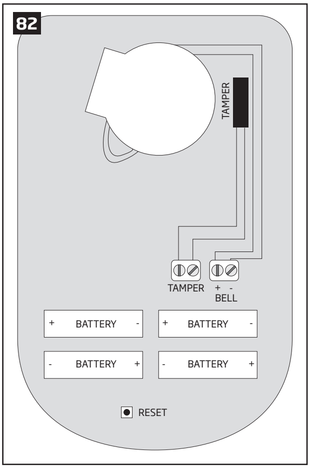
33.7.1. Technical Specifications

33.7.1.1. Electrical & Mechanical Characteristics

Battery type	1,5V Alkaline AA type
Number of batteries	4
Battery operation time	~18 months*
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Range of operating temperatures	-30...+55°C
Dimensions	201 x 140 x 36 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless
Acoustic sound level	~104 dB measured at 1 m

* The operation time depends on different conditions and may vary.

82



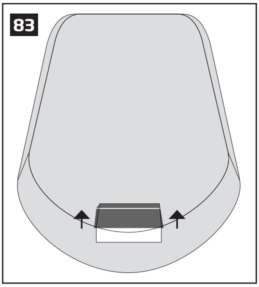
33.7.1.2. Main Unit, LED & Connector Functionality

RESET	Button for restoring default parameters
+ / -	Battery slots
LED indicators	Visual alarm indication
Tamper	Tamper button terminals
Bell+	Positive siren speaker terminal
Bell-	Negative siren speaker terminal

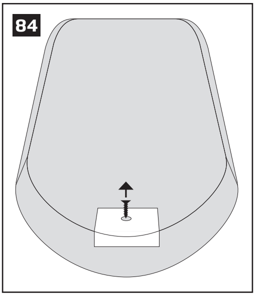
33.7.2. Installation

1. Open EWS2 enclosure.

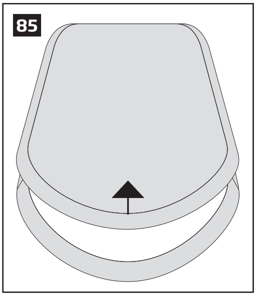
83



84



85



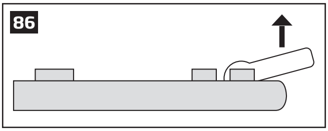
Remove the small blue lid located on the front side of the enclosure by pulling the lid up.

Unscrew the front side of the enclosureю

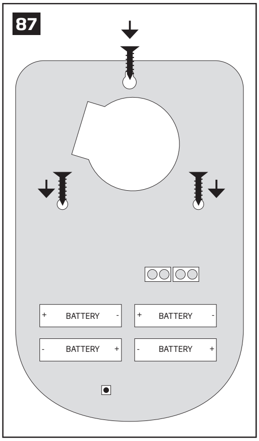
Detach the front side of the enclosure by pulling the front side upю

2. Once the enclosure is opened, remove the plastic tab inserted between one of the battery terminal and battery slots.

86



3. Fix the siren on the wall using the screws.



4. Close EWS2 enclosure.
5. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWS2 closer to alarm system device and bind it again.
7. EWS2 siren is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.7.6. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM364 system can be 0,5 meters.

33.7.3. EWS2 Zone, PGM Output & Tamper

Upon successful EWS2 outdoor siren binding process,the system adds 1 wireless Instant zone and 1 wireless Siren PGM output. The wireless zone is intended for EWS2 tamper control and the wireless PGM output is for siren control.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWS2:

- **By tamper button.** EWS2 has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EWS2 is illegally opened, the tamper button becomes unpressed (see Fig. No. 82). This action is followed by alarm which is sent by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWS2 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS message contains the wireless device model, wireless ID code and tamper number.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

ATTENTION: The siren will sound only if wireless zone of the siren is assigned to the same partition as the one that has been alarmed (see **23.1. Zone Partition**).

33.7.4. Battery Replacement

1. Open EWS2 enclosure.
2. Remove all 4 old batteries from the battery slots.
3. Postition the 4 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWS2
4. Insert the batteries into the battery slots.
5. Batteries replaced.

For more details, please refer to **33.7.2 Installation**.

ATTENTION: Only 1,5V Alkaline AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool software*.

33.7.5. Restoring Default Parameters

1. Remove any battery from EWS2.
2. Press and hold the RESET button.
3. Insert the battery back to EWS2.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

33.8. EW1B - Battery-Powered Wireless Zone & PGM Output Expansion Module

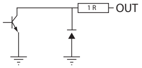
Main EW1B features:

- 2 zones for wired sensor connection;
- 2 PGM outputs for electrical appliance connection.

Wireless expansion module EW1B is a wireless device with 2 zones and 2 PGM outputs. This expansion module connects to ELDES wireless alarm systems and enables wireless access for to 2 wired devices such as movement PIR sensors, magnetic door contacts etc. In addition it allows to connect and control up to 2 appliances, i.e. lighting, heating etc. After the wiring process to EW1B it is necessary to bind EW1B to the alarm system by sending a corresponding command via SMS text message or using software *ELDES Configuration Tool*. t is possible to connect up to 32 EW1B devices to ESIM364 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

33.8.1. Technical Specifications

33.8.1.1. Electrical & Mechanical Characteristics

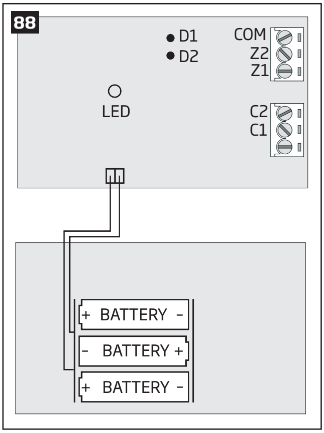
Battery type	1,5V Alkaline AA type
Number of batteries	3
Battery operation time	~18 months*
Number of zones	2
Zone connection type	Normally closed (NC)
Number of PGM outputs	2
EW1B PGM output circuit	 Open Collector Output. Output is pulled to COM when turned ON.
Maximum commuting pgm output values	Voltage – 30V; current 500mA
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless
Range of Operating Temperatures	-20...+55°C
EW1B PCB Dimensions	38x60x12mm
EW1B Enclosure Dimensions	90x110x40mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Enclosure rating	IP65

* The operation time depends on different conditions and may vary.

33.8.1.2. Connector & LED Functionality

COM	Common terminal for zones
Z2, Z1	Security zone terminals
C2, C1	PGM output terminals
D1, D2	Pins for restoring default parameters
LED	EW1B status

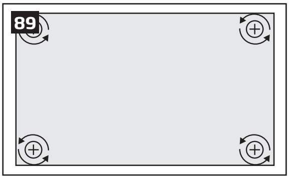
88



33.8.2. Installation

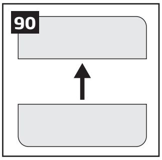
1. Push down the screwdriver and turn it counter-clockwise to unscrew EW1B enclosure.

89



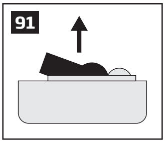
2. Detach the front side of the enclosure by pulling the front side up.

90



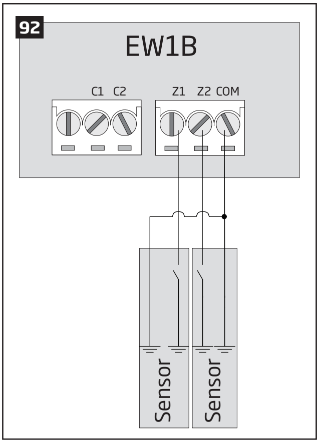
3. Remove the plastic tab inserted between one of the battery terminals and battery slot terminals.

91



4. Connect the circuit as indicated below.

92



6. Close EW1B enclosure.
7. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
8. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EW1B closer to alarm system device and bind it again.

9. EW1B is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.8.5. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM364 system can be 0,5 meters.

33.8.3. EW1B Zones, PGM Outputs & Tamper

Upon successful EW1B module binding process, the system adds 2 wireless Instant zones intended for wired sensor connection and 2 wireless PGM outputs intended for electrical appliance connection and control. The wireless connection loss between EW1B and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS message contains the wireless device model, wireless ID code and tamper number.

33.8.4. Battery Replacement

1. Open EW1B enclosure.
2. Remove all 3 old batteries from the battery slots.
3. Postition the 3 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals as indicated.
4. Insert the batteries into the battery slots.
5. Batteries replaced.

For more details, please refer to **33.8.2. Installation**.

ATTENTION: Only 1,5V Alkaline AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool software*.

33.8.5. Restoring Default Parameters

1. Remove any battery from EW1B.
2. Short circuit (connect) pins D1 and D2.
3. Insert the battery back to EW1B.
4. Wait untill LED provides several short flashes.
5. Remove short-circuit from D1 and D2 pins.
6. Parameters restored to default.

33.9. EWF1 - Wireless Smoke Detector

Main EWF1 features:

- Photoelectric sensor for slow smouldering fires
- TEST button
- Non-radioactive technology for environmental friendly
- High and stable sensitivity
- Quick fix mounting plate for easy installation
- LED operation indicator
- Built-in speaker for audio alarm indication
- Auto-reset when smoke clears

EWF1 is a wireless photoelctric type smoke detector intended to use with ELDES wireless alarm systems. Photoelectric smoke detectors are generally more effective at detecting smouldering fires which smoulder for hours before bursting into flame. An optical method is used for the detection of visible smoke. When the concentration of smoke in the optical chamber exceeds a given threshold, EWF1 sounds the alarm and sends out a signal to the ESIM364 alarm system using the wireless connection and the system triggers the alarm. By default, when more than one EWF1 device is used, the system will automatically activate the interconnection feature (see **20.6. Interconnection**). ESIM364 system support up to 32 EWF1 devices, The maximum wireless connection range is 150 meters (in open areas).

33.9.1. Technical Specifications

33.9.1.1. Electrical & Mechanical Characteristics

Detection type	photoelectric chamber
Detector lifetime	up to 10 years**
Alarm sound level	85 Decibels at 3 meters
Battery voltage	9V
Battery type	6LR61 alkaline
Number of batteries	1
Battery operation time	~18 months*
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Range of operating temperatures	5ºC to 45ºC
Humidity	0-90% RH @ 0… +40 °C (non-condensing)
Sensitivity to smoke	3.0-6.0 % Obs /m
Dimensions	110mm Ø
Compatible with alarm systems	eLDES Wireless
Acoustic sound level	~98 dB measured at 1 m

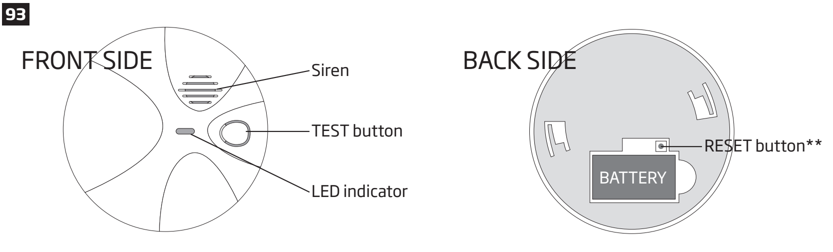
* The operation time depends on different conditions and may vary.

** For more details regarding date of replacement, please refer to the label located on the back side of the device.

33.9.1.2. Main Unit & LED Functionality

TEST	Button for testing / button for testing and restoring default parameters (if RESET button not available)
LED	EWF1 status indication
SIREN	Built-in speaker for audio alarm indication
RESET**	Button for restoring default parameters

93



** Unavailaible on some EWF1 models

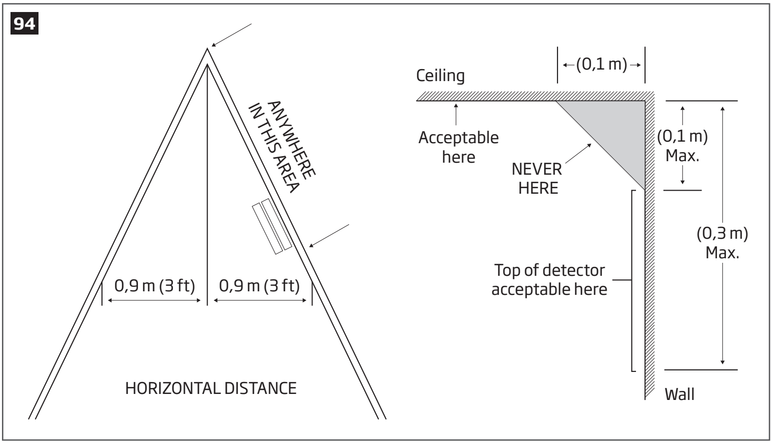
33.9.2. PLACEMENT

1. Install the wireless smoke detector as close to the center of the ceiling as possible. If this is not practical, mount no closer than 10 centimeters from a wall or corner. Also, if local codes allow, install wireless smoke detectors on walls, between 10 and 30 centimeters from ceiling/wall intersections.
2. Install a minimum of two wireless smoke detectors in every house, no matter how small the house is.
3. Install a wireless smoke detector in each room that is divided by a partial wall (either coming down from the ceiling at least 20 centimeters, or coming up from the floor).
4. Install a wireless smoke detector in lived-in attics or attics which ho use electrical equipment like furnaces, air conditioners, or heaters.

NOTE: For best protection we recommend that you install a wireless smoke detector in every room.

Recommended EWF1 placement locations

94

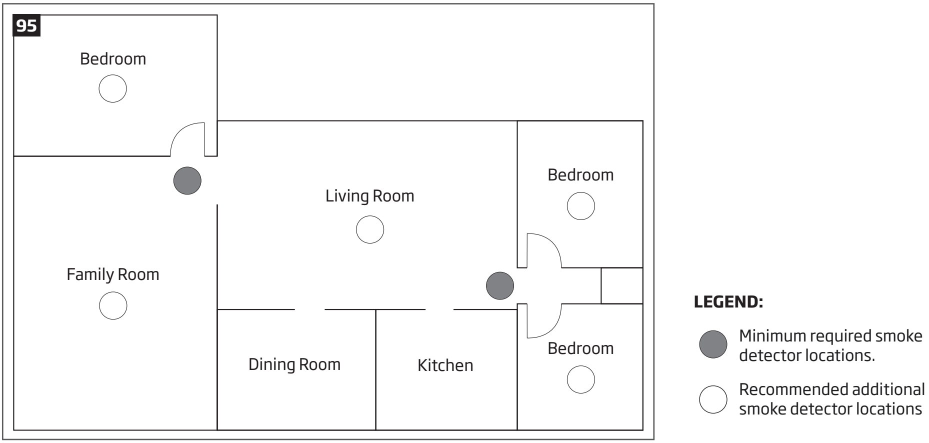


NOTE: Measurements shown are to the closest edge of the detector.

Typical Single-Story House

Install a wireless smoke detector on the ceiling or wall inside each bedroom and in the hallway outside each separate sleeping area. If a bedroom area hallway is more than 9 meters long, install a wireless smoke detector at each end.
If there is a basement: Install a wireless smoke detector on the basement ceiling at the bottom of the stairwell.

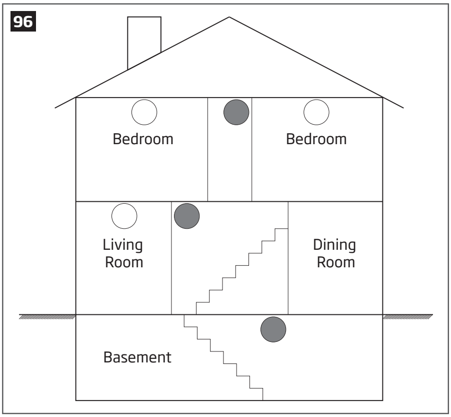
95


Bedroom
Living Room
Bedroom
Family Room
Bedroom
Dining Room
Kitchen
LEGEND:
Minimum required smoke detector locations.
Recommended additional smoke detector locations

Typical Multi-Story or Split-Level House

Install a wireless smoke detector on the ceiling or wall inside each bedroom and in the hallway outside each separate sleeping area. If a bedroom area hallway is more than 9 meter long, install a wireless smoke detector at each end. Please install a wireless smoke detector on the top of a first-to-second floor stairwell.

96



LEGEND:

● Minimum required smoke detector locations.

○ Recommended additional smoke detector locations

Incorrect EWF1 Placement

DO NOT place EWF1 in the following locations:

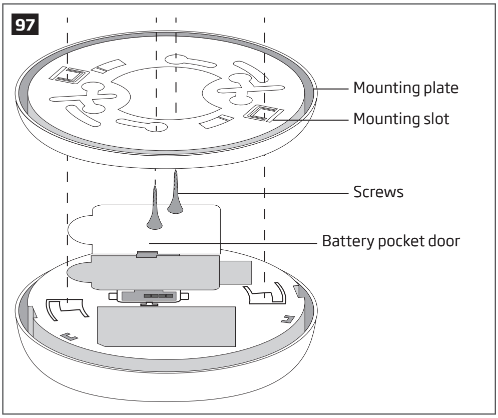
- Near appliances or areas where normal combustion regularly occurs (kitchens, near furnaces, hot water heaters). Use specialized wireless smoke detector with unwanted alarm control for this areas.
- In areas with high humidity, like bathrooms or areas near dishwashers or washing machines. Install at least 3 meters away from these areas.
- Near air returns or heating and cooling supply vents. Install at least 1 meter away from these areas. The air could blow smoke away from the detector, interrupting its alarm.
- In rooms where temperatures may fall below 5°C or rise above 45°C.
- In extremely dusty, dirty, or insect-infested areas where loose particles interfere with wireless smoke detector operation.

ATTENTION: Incorrect placement will result in a decrease of operational effectiveness.

33.9.3. Installation

1. Detach the mounting plate by turning it counter-clockwise from the back of EWF1 (see Fig. No. 97).
2. Secure the mounting plate to ceiling or wall with mounting screws.(see Fig. No. 97).
3. Lift to open the battery pocket door (see Fig. No. 97).
4. Insert the battery into the battery pocket considering the polarity terminals indicated on the enclosure of EWF1. Ensure the battery is securely connected. Red LED may flash briefly when the battery is being installed.
5. Close the battery pocket door by snapping it into place.
6. Position the smoke detector to the mounting plate by turning it clockwise to lock into place. Note that the device will not lock into the mounting plate without the battery being present in the battery pocket.
7. Push the TEST button to verify if the wirless smoke detector is operational. See **33.9.5.1. Testing EWF1.**
8. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWF1 closer to alarm system device and bind it again.
10. EWF1 wireless smoke detector is ready for use.

97



NOTE: If you are unable to bind the wireless device, please restore the parameters of the wireless device to default and try again. See chapter **33.9.6. Restoring Default Parameters** for more details.

33.9.4. Interconnection

The interconnection feature automatically links all wireless smoke detectors resulting in causing an instant alarm in the system along with the rest of EWF1 wireless smoke detectors. For more details on interconnection feature and how to manage it, please refer to **20.4. EWF1 Interconnection.**

33.9.5. Maintenance

33.9.5.1. Testing EWF1

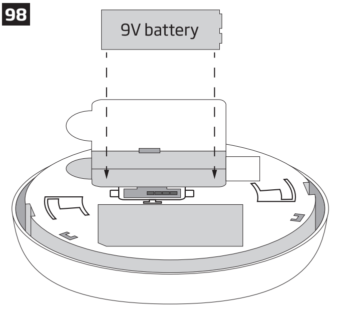
- The TEST button verifies if EWF1 is operational. Firmly push the TEST button and the wireless smoke detector will sound a loud beep. The alarm will stop sounding after releasing the TEST button. When testing EWF1 using *ELDES Configuration Tool* software, the detector will provide short beeps.
- Stand at arm's length from the wireless smoke detector when testing.
- Test wireless smoke detectors weekly and upon returning from vacation or when no one has been in the household for several days.
- Test each wireless smoke detector to be sure it is installed correctly and operating properly.
- DO NOT use an open flame to test this wireless smoke detector. You may ignite and damage the wireless smoke detector or your home.
- If the wireless smoke detector does not sound, please check the battery and signal level using *ELDES Configuration Tool* software.

ATTENTION: Test all wireless smoke detectors weekly to ensure proper operation.

33.9.5.2. Battery Replacement

1. Turn EWF1 counter-clockwise to detach it from the mounting plate.
2. Gently pull down the wireless smoke detector.
3. Remove the old battery from the battery pocket.
4. Postition the new 9V battery according to the appropriate battery slot positive/negative terminals indicated on the enclosure of EWF1. Ensure the plastic battery holder is fully depressed when the battery has been fitted.
5. Using the TEST button, test the wireless smoke detector to verify if it is operational. See **33.9.5.1. Testing EWF1.**
6. Re-attach the wireless smoke detector to the mounting plate by turning the wireless smoke detector clockwise until it snaps into place.

98



ATTENTION: Only 9V 6F22 primary alkaline type battery can be used. Install only new, high quality and unexpired batteries.

ATTENTION: The battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

NOTE: The system sends an SMS message to the preset user phone number as soon as the battery level runs below 5%.

33.9.6. Restoring Default Parameters

1. Remove the battery from EWF1.
2. Press and hold the RESET button.
3. Insert the battery back to EWF1.
4. Hold the RESET button until you hear a short beep.
5. Release the RESET button.

On some EWF1 models the RESET button is not available. On such EWF1 devices the reset process is as follows:

1. Remove the battery from EWF1.
2. Wait for 1 minute or more.
3. Press and hold the TEST button.
4. Insert the battery back to EWF1.
5. Hold the TEST button for 10 seconds or more.
6. Release the TEST button.

ATTENTION: EWF1 built-in speaker will sound while pressing and holding the TEST button. Please, ignore the sound.

33.9.7. Cleaning

Clean the wireless smoke detector at least once a month to remove dust, dirt, or debris. Using the soft brush or wand attachment of a vacuum cleaner, vacuum all sides and cover of wireless smoke detector. Be sure all the vents are free of debris.
If necessary, use a damp cloth to clean wireless smoke detector cover.

NOTE: Do not attempt to remove the cover to clean inside the wireless smoke detector. This will void your warranty.

33.10. EWK2/EWK2A - Wireless Keyfob

Main Features:

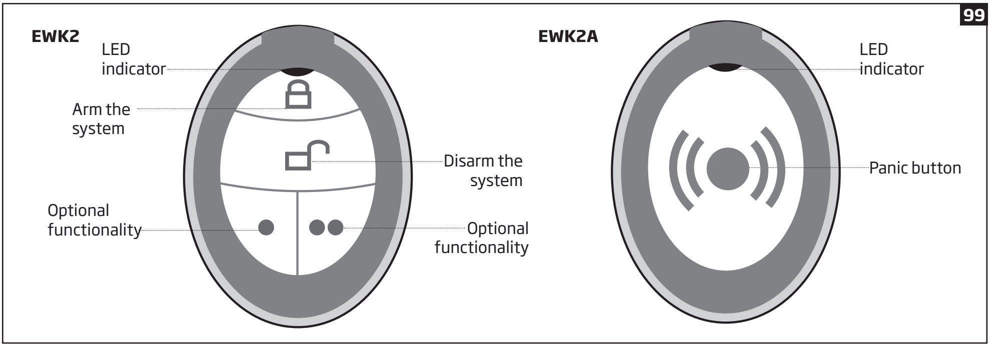
- Alarm system arming & disarming;
- Panic button;
- PGM output control;
- Visual and audio indication of command status.

For more details, please refer to ELDES alarm system user and installation manuals.

EWK2/EWK2A is a wireless device intended to remotely arm and disarm ELDES alarm system, cause system alarm (Panic Button) or to control any electric appliance connected to the alarm system's PGM output. In order to start using wireless keyfob EWK2/EWK2A, it has to be bound to ELDES wireless alarm system using *ELDES Configuration Tool* software or sending a corresponding SMS text message. EWK2 keyfob features four configurable buttons intended to operate according to individual needs,while EWK2A keyfob model features one configurable button. After the button is pressed, EWK2/EWK2A internal buzzer's sound signal and red LED indicator confirms a transferred command to ELDES alarm system via wireless connection. The status of the sent command can be checked by attempting to receive the feedback signal from the alarm system. This can be performed by pressing down the same button again and holding it for 3 seconds. 3 short sound signals and LED indicator flashes indicate a successfully carried out command, while 1 long beep and LED indicator flash stands for failed command and feedback signal failure. By default, one pair of buttons is already configured to arm and disarm the alarm system.

It is possible to connect up to 5 EWK2/EWK2A devices to ELDES alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

33.10.1. Technical specifications



NOTE: the picture above reflects the default EWK2/EWK2A button configuration. All EWK2 keyfob buttons are/EWK2A keyfob button is configu-rable according to individual needs.

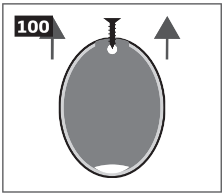
33.10.1.1. Electrical & Mechanical Characteristics

Battery type	CR2032 Lithium
Battery voltage; capacity	3V; 240 mAh
Quantity of batteries	1
Battery operation time	~18 months*
Wireless transmitter-receiver frequency	868 Mhz
Range of operating temperatures	-20...+55°C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Dimensions	53 x 37 x 10 mm
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless

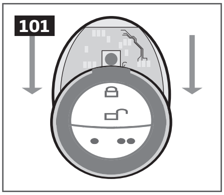
* This operation time can be achieved by pressing the keyfob button up to 4 times per day. The operation time depends on different conditions and may vary.

33.10.2. Installation

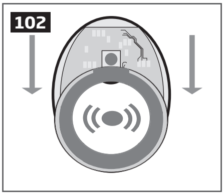
1. Remove the screw located on the back side of EWK2/EWK2A enclosure.



2. Once the enclosure is opened, remove the PCB from the EWK2/EWK2A enclosure and flip the PCB so that the back side would be facing up.

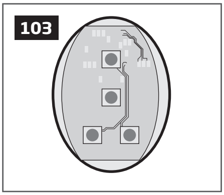


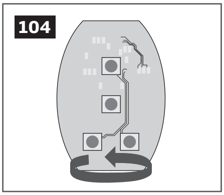
EWK2



EWK2A

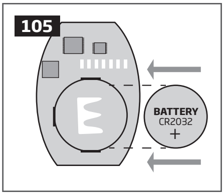
3. Insert the CR2032 type battery provided in the EWK2/EWK2A pack. Before inserting the battery, ensure that it is positioned plus-marked side up.





4. Insert the CR2032 type battery provided in the EWK2/EWK2A package. Before inserting the battery, ensure that it is positioned plus-marked side up.

105



5. Insert the PCB back to the enclosure and close it.
6. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
7. Press any EWK2 button/press the EWK2A button several times until the device is successfully bound.
8. EWK2/EWK2A is ready for use.

NOTE: If you are unable to bind the wireless device, please, restore the parameters of the wireless device to default and try again. See chapter **33.10.5. Restoring Default Parameters** for more details.

33.10.3. Panic Button

by default, EWK2A keyfob supports a Panic Button feature allowing to cause an alarm at any time when the keyfob button is pressed. EWK2 keyfob may support a Panic Button feature. This feature that can be configured using *ELDES Configuration Tool* software by creating a virtual zone of Panic/Silent or 24-Hour type and assigning it to Virtual Alarm option. The Panic Button feature can be set up on any button of EWK2.

33.10.4. Battery Replacement

1. Open EWK2/EWK2A enclosure.
2. Remove the old battery from the battery slot.
3. Postition the new battery according to the appropriate battery slot positive terminal indicated.
4. Insert the battery into the battery slot.
5. Battery replaced.

See **33.10.2 installation** for more details.

ATTENTION: Only CR2032 3V battery can be used. Install only new, high quality and unexpired batteries.

ATTENTION: The battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

33.10.5. Restoring Default Parameters

EWK2

1. Press and hold ● and ●● buttons simultaneously.
2. Hold the buttons pressed until LED indicator and the buzzer provide several short flashes and beeps simultaneously.
3. Release the buttons.
4. Parameters restored to default.

EWK2A

1. Press and hold the lower side of the button. ((●))
2. Hold the button pressed until LED indicator and the buzzer provide several short flashes and beeps simultaneously.
3. Release the button.
4. Parameters restored to default.

33.11. EWD2 - Wireless Door Contact/Shock Sensor/Water Sensor

Main EWD2 features:

- Built-in shock sensor
- 2 wireless zones
- Available zone modes: magnetic door contact, shock sensor, water sensor, digital sensor
- 2 built-in tamper switches: on the front and on the back of the PCB

EWD2 is a wireless device intended to secure doors, windows or any other opening/clsoing mechanisms. In addition, the device comes equiped with a built-in shock sensor for vibration detection, an on-board zone terminal designed for external digital sensor or water sensor connection and 2 built-in tamper switches for EWD2 sabotage detection. In order to start using EWD2, it has to be bound to ELDES alarm system using *ELDES Configuration Tool* software or by sending a corresponding SMS text message to ELDES alarm system.

It is possible to connect up to 32 WD2 devices to ESIM364 alarm system. The maximum wireless connection range is 150 meters (in open areas).

33.11.1. Technical Specifications

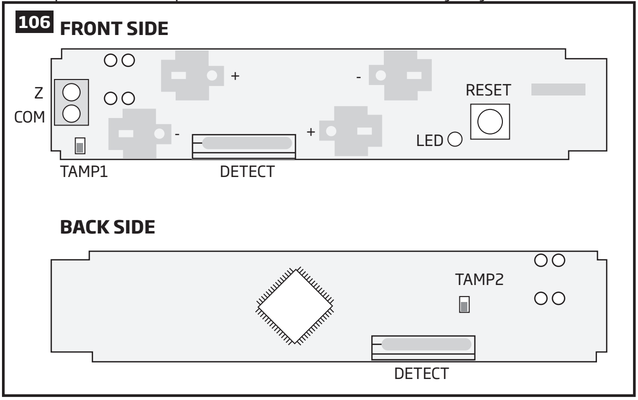
33.11.1.1. Electrical & Mechanical Characteristics

Batteries	1,5V Alkaline AAAA type, LR8 (IEC standard) / 25A (ANSI/NEDA standard)
Number of batteries	2
Battery operation time	~18 months*
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Wireless communication range	Up to 30 meters in premises; up to 150 meters in open areas
Range of operating temperatures	-20...+55°C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
EWD2 dimensions	101 x 22 x 20 mm
Magnet dimensions	47 x 17 x 10 mm
Compatible with alarm systems	ELDES Wireless

33.11.1.2. Main Unit and LED Functionality

* The operation time depends on different conditions and may vary.

106



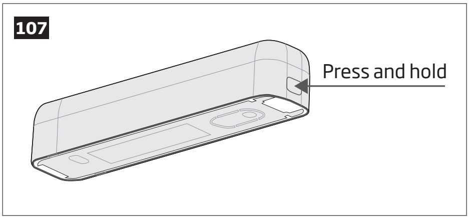
Unit	Description
Z	Zone terminal
COM	Common terminal
TAMP1	Tamper switch
+ / -	Battery slots
DETECT	Magnet detector
LED	Light-emitting diode for indication of parameter restoring to default
RESET	Button for restoring default parameters
TAMP2	Tamper switch

ATTENTION for EWD2 v1 and EWD2 v2: If no sensor is to be connected to EWD2 on-board zone terminal, please make a short-circuit (connect) Z and COM terminals in order to avoid the unnecessary battery power usage.

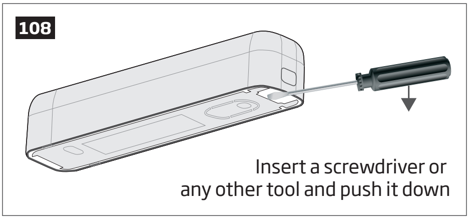
33.11.2. Installation

1. Remove the cover of EWD2 enclosure.

107

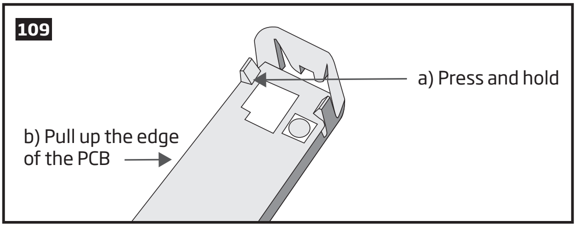


108



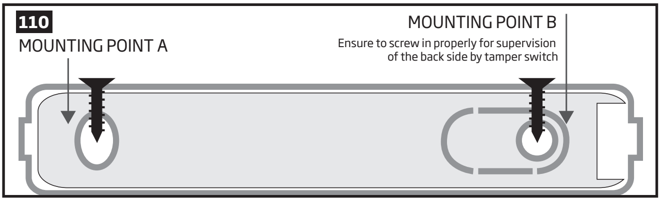
2. Remove the PCB (printed-circuit-board) from the enclosure.

109



3. Screw in the enclsoure to the door or window jamb.

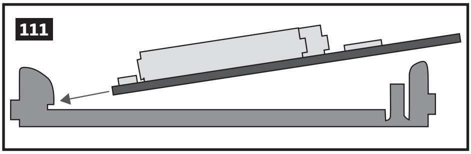
110


MOUNTING POINT A
MOUNTING POINT B
Ensure to screw in properly for supervision
of the back side by tamper switch

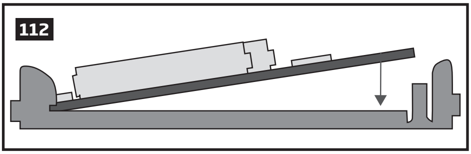
4. Wire up the external digital sensor (if any) or water sensor (if any) to Z and COM terminals, otherwise do not perform any wiring.

5. Insert the PCB back into the enclosure

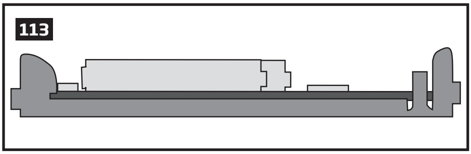
111



112

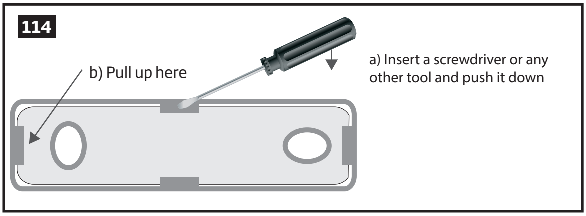


113



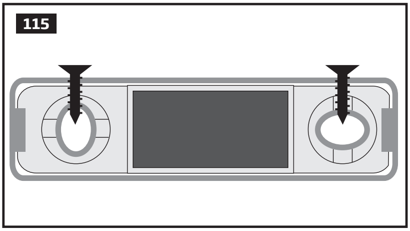
6. Remove the cover of the magnet enclosure.

114

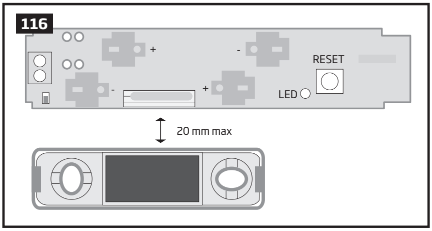


7. Screw in the magnet to the door or window frame and ensure that the magnet is fixed at the same height as the EWD2 magnet detector.

115



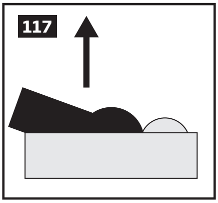
116



8. Cover the magnet. No tools are required for this action.

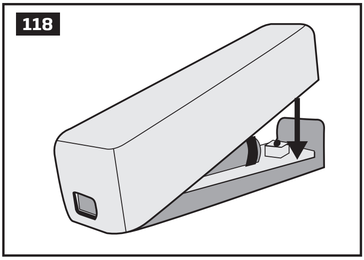
9. Remove the plastic tab inserted between one of the battery terminals and battery slots of EWD2.

117



10. Close EWD2 enclosure. Insert the cover to the left edge of the enclosure's bottom part and push the cover down. DO NOT use any tools for this action.

118



ATTENTION: DO NOT attempt to close EWD2 enclosure the other way round, otherwise you might break it.

11. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.

12. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWD2 closer to alarm system device and bind it again.

13. EWD2 is ready for use.

ATTENTION: Ensure that EWD2 device is properly fixed to the wall and the Mounting Point B portrayed in Fig. No. 110 is properly screwed in. Otherwise, the tamper switch will NOT supervise the back side of EWD2 enclosure (see also **33.11.3. EWD2 Zones and Tampers**).

NOTE: If you are unable to bind the wireless device, please, restore the parameters of the wireless device to default and try again. See **33.11.5. Restoring Default Parameters** for more details.

33.11.3. EWD2 Zones and Tampers

Upon successful EWD2 magnetic door contact binding process, the system adds 2 wireless Instant zones. The wireless zones can be set up to operate under one of the following modes each:

- **Zone 1:**
  - **Magnetic door contact** – Designed for causing an alarm (by default) if doors/windows are opened when the system is armed.
  - **External sensor** – Designed for causing an alarm (by default) if the wired digital sensor, connected to Z and COM terminals, is triggered when the system is armed. This mode does NOT operate with *Water sensor* mode on Zone 2 simultaneously.
- **Zone 2:**
  - **Shock sensor** – Designed for causing an alarm (by default) if the built-in shock sensor is triggered.
  - **Water sensor** – Designed for causing an alarm (by default) if a water sensor, connected to Z and COM terminals, is triggered. This mode does NOT operate with External sensor mode on Zone 1 simultaneously.

Possible zone mode combinations:

- **Zone 1:** Magnetic door contact + **Zone 2:** Shock sensor
- **Zone 1:** Magnetic door contact + **Zone 2:** Water sensor
- **Zone 1:** External Sensor + **Zone 2:** Shock sensor
- **Zone 1:** Magnetic door contact + **Zone2:** N/A
- **Zone 1:** External Sensor + **Zone2:** N/A
- **Zone 1:** N/A + **Zone 2:** Shock sensor
- **Zone 1:** N/A + **Zone 2:** Water sensor

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWD2:

- **By tamper switch.** EWD2 comes equipped with 2 built-in tamper switches intended for enclosure supervision:
  - one located on the front side of the PCB supervising the front cover in case it is illegally opened (see Fig. No. 106).
  - the other one located on back of the PCB supervising the back side of the enclosure in case the EWD2 is illegally detached from the wall (see Fig. No. 106).

  Once the enclosure of EWD2 is tampered, the tamper switch will become triggered. This action will be followed by alarm, resulting in sending an SMS text message and/or phone call to the user. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWD2 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS
- message contains the wireless device model, wireless ID code and tamper number.

ATTENTION: The tamper will not operate if both wireless zones are disabled.

For more details on EWD2 zone and tamper configuration, please refer to *ELDES Configuration Tool* software's HELP section.

33.11.4. Battery Replacement

1. Open EWD2 enclosure.
2. Remove both old batteries from the battery slots.
3. Insert the 2 new 1,5V Alkaline AAAA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB of EWD2.
4. Batteries replaced.

See **33.11.2. Installation** for more details.

ATTENTION: Only 1,5V Alkaline AAAA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

ATTENTION: The system sends an SMS message to a preset user phone number as soon as the battery level runs below 5%.

ATTENTION: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

33.11.5. Restoring Default Parameters

1. Remove any battery from EWD2.
2. Press and hold the RESET button.
3. Insert the battery back to EWD2.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

33.12. EWS3 - Wireless Indoor Siren

Main features:

- Audio alarm indication by 2 built-in speakers.
- Visual alarm indication by built-in LED indicators: burglary/24-hour/tamper alarm and fire alarm indicated in different colours.
- 2 tamper switches: for enclosure opening and device detachment from the wall detection.

EWS3 is a wireless indoor device with built-in siren speakers and LED indicators operating with ELDES wireless alarm systems. The device is designed to notify the user by audio and visual signals in the event of alarm as well as in event of system arming/disarming (Bell Squawk feature must be enabled). In the event of burglary, 24-hour or tamper alarm, EWS3 will activate the speakers and flash the blue LED indicators, while in case of a fire alarm, the device can flash the red LED indicator (both features require EWS3 Alarm LED and EWS3 Fire Alarm LED parameters to be enabled using *ELDES Configuration Tool* software or EKB2/EKB3/EKB3W keypad)

To start using EWS3, it has to be bind to ELDES alarm system by sending a corresponding SMS message or using software *ELDES Configuration Tool*. Upon successful EWS3 binding process, the system adds one wireless zone and one wireless PGM output. In case of alarm, the siren provides a sound alarm for one minute. The configuration of this parameter is disabled for EWS3 in order to save the battery power.

It is possible to connect up to 32 EWS3 devices to ESIM364 alarm system. The maximum wireless connection range is 150 meters (in open areas).

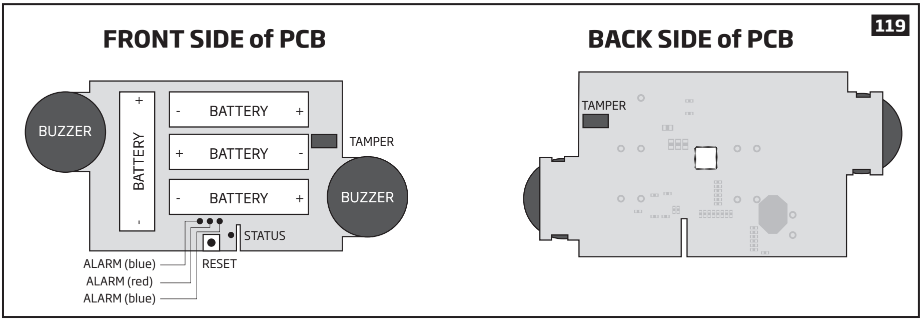
33.12.1. Technical Specifications

33.12.1.1. Electrical & Mechanical Characteristics

Battery type	1,5V Alkaline AA type
Number of batteries	4
Battery operation time	~18 months*
Wireless transmitter-receiver frequency	868 Mhz
Range of operating temperatures	-25...+55°C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Dimensions	167 x 80 x 34 mm
Wirelesscommunication range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with alarm systems	ELDES Wireless
Acoustic sound level	~90 dB measured at 1 m

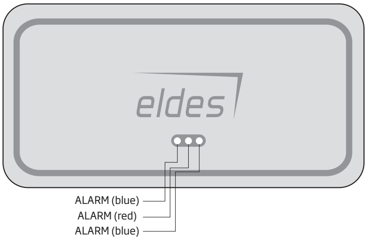
* The operation time might vary in different conditions.

33.12.1.2. Main Unit, LED & Connector Functionality



RESET	Button for restoring default parameters
+ / -	Battery slots
STATUS	LED indicator for data transmission indication
ALARM (blue)	Blue LED indicators for visual alarm indication
ALARM (red)	Red LED indicator for visual alarm indication
BUZZER	Speakers for audio alarm indication
TAMPER	Tamper switches

120 **FRONT SIDE of ENCLOSURE**

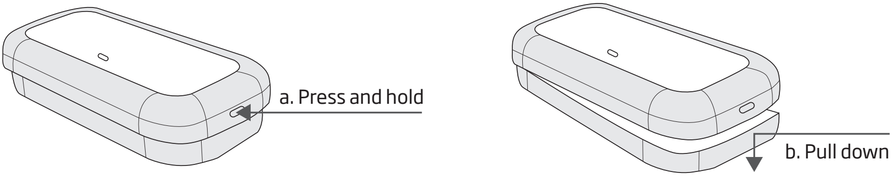


LED indication	Description
ALARM (blue) flashing	Burglary, 24-Hour or tamper alarm in progress
ALARM (red) flashing	Fire alarm in progress

33.12.2. Installation

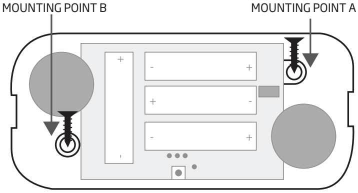
1. open EWS3 enclosure.

121

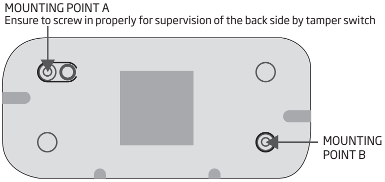


2. Once the enclosure is opened, fix the siren to the wall using the screws.

122

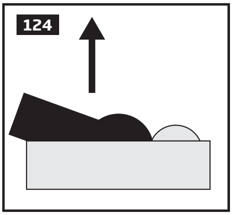


123


MOUNTING POINT A
Ensure to screw in properly for supervision of the back side by tamper switch
MOUNTING POINT B

3. Remove the plastic tab inserted between one of the battery terminals and battery slot contacts.

The wireless connection loss between EWS3 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS
message contains the wireless device model, wireless ID code and tamper number.



4. STATUS indicator should start flashing indicating successful data transmission.
5. Close EWS3 enclosure by putting the cover back.
6. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
7. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWS3 closer to alarm system device and bind it again.

ATTENTION: Ensure that EWS3 device is properly fixed to the wall and the Mounting Point A portrayed in Fig. No. 122 and Fig. No. 123 is properly screwed in. Otherwise, the tamper switch will NOT supervise the back side of EWS3 enclosure (see also 33.12.3. EWS3 Zone, PGM Output and Tamper).

NOTE: If you are unable to bind the wireless device, please, restore the parameters of the wireless device to default and try again. See chapter **33.12.5. Restoring Default Parameters** for more details.

33.12.3. EWS3 Zone, PGM Output and Tamper

Upon successful EWS3 outdoor siren binding process,the system adds 1 wireless Instant zone and 1 wireless Siren PGM output. The wireless zone is intended for EWS3 tamper control and ability to assign a partition (-s), while the wireless PGM output is intended for siren speaker control.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWS3:

• **By tamper switch.** EWS3 comes equipped with 2 built-in tamper switches intended for enclosure supervision:

- one located on the front side of the PCB supervising the front cover in case it is illegally opened (see Fig. No. 119).
- the other one located on back of the PCB supervising the back side of the enclosure in case the EWS3 is illegally detached from the wall (see Fig. No. 119).

Once the enclosure of EWS3 is tampered, the tamper switch will become triggered. This action will be followed by alarm, resulting in sending an SMS text message and/or phone call to the user. The SMS text message contains the violated tamper number.

• **By wireless connection loss.** The wireless connection loss between EWS3 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS message contains the wireless device model, wireless ID code and tamper number.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

33.12.4. Battery replacement

1. open EWS3 enclosure.
2. Remove all 4 old batteries from the battery slots.
3. Postition the 4 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWS3
4. Insert the batteries into the battery slots.
5. Batteries replaced.

See chapter **33.12.2. Installation** for more details.

ATTENTION: Only 1,5V Alkaline AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset user phone number as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

5.12.1. Restoring default parameters

1. Remove one battery from EWS3.
2. Press and hold the RESET button.
3. Insert the battery back to EWS3.
4. Hold the RESET button until LED indicator starts blinking.
5. Release the RESET button.
6. Parameters reset to default.

34. SERVICE MODE

The system comes equipped with Service mode allowing to carry out system maintenance tasks, such as detection device replacement, tamper switch installation, wireless device battery replacement without causing zone or tamper alarm when Service mode is activated. To activate/deactivate Service mode, please refer to the following configuration methods:

Activate Service mode

SMS

SMS text message content:
ssss_SERVICEMODE:ON
Value: *ssss* - 4-digit SMS password.
Example: *1111_SERVICEMODE:ON*

EKB2

Menu path:
OK → iiii → OK → SERVICE MODE → OK → ENABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 67 & parameter status value:
671 #
Example: *671#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software.*

Deactivate Service mode

SMS

SMS text message content:
ssss_SERVICEMODE:OFF
Value: *ssss* - 4-digit SMS password.
Example: *1111_SERVICEMODE::OFF*

EKB2

Menu path:
OK → iiii → OK → SERVICE MODE → OK → DISABLE → OK
Value: *iiii* – 4-digit installer code.

EKB3/ EKB3W

Enter parameter 67 & parameter status value:
670 #
Example: *670#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool software.*

NOTE: Alternatively, the Service mode automatically deactivates when 1-hour timeout period expires or after arming the system.

35. REMOTE SYSTEM RESTART

In some critical situations, a system restart may be required. To remotely carry out system restart, please refer to the following configuration method.

Restart the system

SMS

SMS text message content:
ssss_RESET
Value: *ssss* – 4-digit SMS password.
Example: *1111_RESET*

36. EN 50131-1 GRADE 3

EN50131-1 **GRADE 3**

ESIM364 system complies with EN 50131-1 Grade 3 security standard requirements and comes equipped with the following features:

- 6-digit SMS password, user/master and installer codes.
- Prompt for master and installer codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool software*.
- System arming is blocked if any system fault exists. The user will not be able to arm the system until all existing system faults are solved.
- System arming is blocked until tamper fault is cleared by the installer.

By default, the EN 50131-1 Grade 3 features are disabled. To enable/disable them, pelase refer to the following configuration methods:

Set 6-digit format for SMS password, user/master and installer codes

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set 4-digit format for SMS password, user/master and installer codes

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Prompt for master and installer codes when configuring the system by EKB2, EKB3, EKB3W keypad or *ELDES Configuration Tool software*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Prompt for installer code when configuring the system using *ELDES Configuration Tool software*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Deny system arming if any system fault exists

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Permit system arming if any system fault exists

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Clear tamper fault

EKB2

Menu path:
OK → iiii → OK → CLEAR TAMPER FAULT → OK
Value: *iiii* – 4-digit installer code.

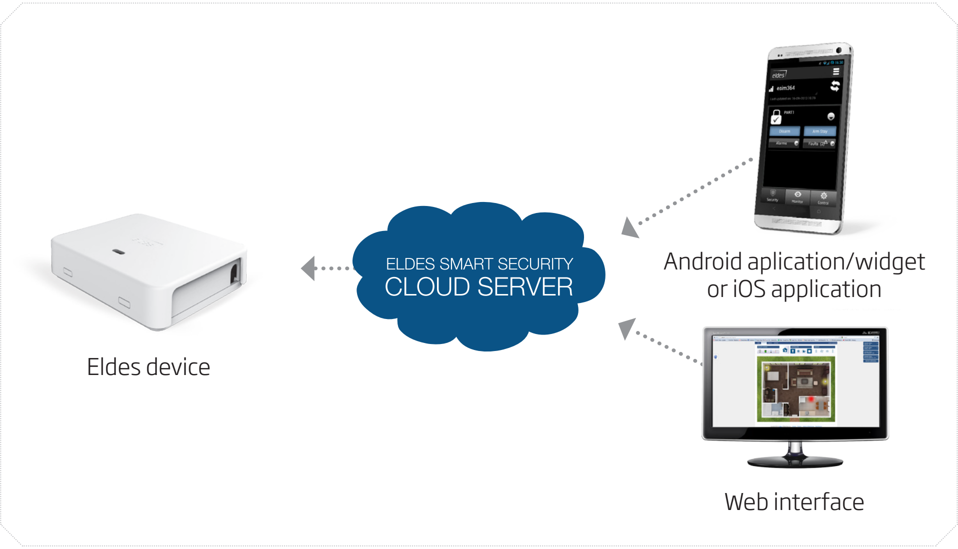
EKB3/ EKB3W

Enter parameter 22:
22 #
Example: *22#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool software*.

37. SMART SECURITY

ELDES Smart Security is a cloud-based platform providing a user-friendly graphical interface intended for system status monitoring and control. The solution consists of:



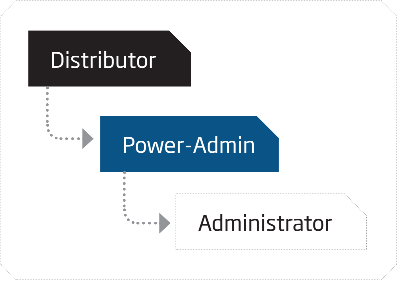
- **ELDES device** – The following ELDES devices come or can be equipped with ELDES Smart Security:
  - ESIM364
  - EPIR2
  - ESIM120
  - any other ELDES device on request
- **Android application/widget and iOS application** – The graphical interface can be accessed via a smart-phone application developed for Android and iOS-based (iPhone, iPad) devices.
- **Web interface** – ELDES Smart Security grants access to the device configuration (ESIM120) and user administration options as well as all features mentioned above when accessed via a web-browser.
- **ELDES Smart Security cloud server –** The server links all ELDES Smart Security components to each other.

ELDES Smart Security solution allows to perform the following*:

- Arm/disarm the system
- Control gates or any other electric appliance connected to the output of the ELDES device
- View system faults and alerts
- Monitor GSM signal strength, back-up battery level and temperature
- Configure ELDES device

* - depends on the ELDES device in use. For more details on the available features, please refer to ELDES device user manual.

User hierarchy



For more details on Smart Security solution, please refer Smart Security manual located at www.eldes.lt/download

38. TECHNICAL SUPPORT

38.1. Troubleshooting

Indication	Possible reason
Indicator STAT is off	· No main power supply · Wiring done improperly · Blown fuse
Indicator NETW is off or flashing	· Missing SIM card · PIN code is enabled · SIM card is inactive · Disconnected antenna · GSM network signal too weak · Problems with GSM provider · Microcontroller is not started due to electrical mains noise or static discharge
System does not send any SMS text messages and/or does not ring	· SIM card credit balance depleted · Incorrect SMS centre phone number · No GSM network signal · User number is not added (or control from anu phone number is disabled) · SIM card changed before disconnecting main power supply or backup battery
Received SMS text message "Wrong syntax"	· Incorrect SMS text message structure · Extra space symbol could be left in SMS text message
Missing temperature indication in Info SMS text message/EKB2 keypad	· Temperature sensor not connected · Temperature sensor broken · Connection wires too long
24H and/or *Fire* zones do not work	· Specified zone must be enabled by SMS, *ELDES Configuration Tool*, EKB2, EKB3 or EKB3W
No sound during remote listening	· Microphone not connected · Improper microphone connection

For product warranty repair service please , contact your local retail store where this product was purchased.
If your problem could not be fixed by the self-guide above, please contact your local distributor. More up to date information about your device and other products can be found at the manufacturer's website www.eldes.lt

38.2. Restoring Default Parameters

1. Disconnect the power supply and backup battery.
2. Short circuit (connect) DEF pins.
3. Power up the device for 7 seconds.
4. Power down the device.
5. Remove short circuit from DEF pins.
6. Parameters restored to default.

38.3. Updating the Firmware via USB Cable Locally

1. Disconnect the power supply and backup battery.
2. Short circuit (connect) DEF pins.
3. Connect the device via USB cable to the PC.
4. Power up the device.
5. The new window must pop-up where you will find the .bin file. Otherwise open *My Computer* and look for *Boot Disk* drive.
6. Delete the .bin file found in the drive.
7. Copy the new firmware .bin file to the very same window.
8. Power down the device.
9. Unplug USB cable.
10. Remove short circuit from DEF pins.
11. Power up the device.
12. Firmware updated.

NOTE: It is strongly recommended to restore default parameters after the firmware update.

38.4. Updating Firmware via GPRS Connection Remotely

ATTENTION: The system will NOT send any data to monitoring station while updating the firmware remotely via GPRS network. However, during the firmware update process, the data messages are queued up and transmitted to the monitoring station after the firmware upgrade process is over.

Before updating the firmware remotely via GPRS connection, make sure that:

- SIM card is inserted into SIM CARD1 slot of ESIM364 device (see **2.2. Main Unit, LED & Connector Functionality**).
- Mobile internet service (GPRS) is enabled on the SIM card.
- Power supply is connected to ESIM364.
- Default SMS password is changed to a new 4-digit password (see **6. SMS PASSWORD AND INSTALLER CODE**).
- At least User 1 phone number is set up (see **8. USER PHONE NUMBERS**).
- APN, user name and password are set up (see **30.2.1. GPRS Network and ELAN3-ALARM**).

Initiate FOTA

ESIM364 alarm system supports FOTA (firmware-over-the-air) feature. This allows to upgrade the firmware remotely via GPRS connection. Once the upgrade process is initiated, the system connects to the specified FTP server address where the firmware file is hosted and begins downloading and re-flashing the firmware. The firmware file must be located in a folder titled **Firmware**. In order to initiate the upgrade process please , send the following SMS message.

SMS

SMS text message content:
XXXX_FOTA:ftp-server-ip,port,firmware-file-name.bin,user-name,password

Value: *ssss* - 4-digit SMS password; *ftp-server-io* - public IP address of FTP server where EPIR firmware file is stored; *port* - port number of FTP server (usually - 21); *firmware-file-name.bin* - name of the firmware file, allowed max. length - up to 31 character; *user-name* - user name of FTP server login, allowed max. length - up to 31 character; *password* - password of FTP server login, allowed max. length - up to 31 character.
Example: *1111_FOTA:84.15.143.111,21,ESIM364fw bin,eldesuser,eldespassword*

ATTENTION: *Comma* character is NOT allowed to use in user name and firmware file name.

ATTENTION: "ELDES UAB" does not run a FTP server and does not host the firmware files online. Please, contact your local distributor to request the latest firmware file: support@eldes.lt

NOTE: It is strongly recommended to restore default parameters after the firmware update.

38.5. Frequently Asked Questions

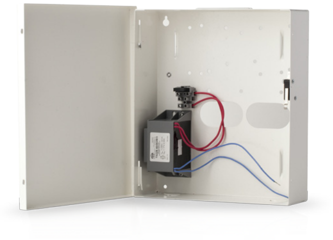
Question	Answer
1. Can ESIM364 operate as standalone device without SIM card inserted?	Yes, ESIM364 device can fully operate without any SIM card inserted. In this case you will not be able to configure and control the device by SMS and calls nor to receive any SMS reports and calls.
2. I am unable to arm the alarm system when one of the zones (some zones) is violated, although I was able to perform disarming. Is there a way to arm the alarm system while the zone is violated?	Due to security reasons it is recommended to restore the violated zone (-s) before arming the alarm system. However, you can enable a Force attribute or use the Bypass feature in order to arm the alarm system despite the violated zone (-s) being present. Please, refer to **14.5. Zone Type Definitions** and **14.7. Bypassing and Activating Zones**.
3. I have activated ATZ mode in *ELDES Configuration Tool* software, but I am unable to set the connection Type 5. Whenever I select Type 5 and press the "Write Settings" button it switches back to Type 4. What's wrong?	It appears that your *ELDES Configuration Tool* software is outdated. Please, download the latest *ELDES Configuration Tool* software version by visiting www.eldes.lt/en/download.
4. When ESIM364 fully powers down my configuration becomes lost and I have to re-configure the device again. What's wrong?	This might have happened due to the jumper left on DEF pins or it is a hardware failure. Please, remove the jumper if it is present on DEF pins or contact your supplier for warranty service.
5. I have a smoke detector connected to ESIM364 system. How do I reset the smoke detector when the "Fire" zone is violated?	If the smoke detector is connected to one of the ESIM364 PGM outputs you can reset it by turning the PGM output OFF and then back ON. This can be performed by SMS, EKB2 keypad, EKB3 keypad, EKB3W keypad and *ELDES Configuration Tool* software. Please, refer to **18.4. Turning PGM Outputs ON and OFF**.
6. What happens if I switch backup battery pole terminals places?	Switching backup battery pole terminals places is forbidden. Otherwise this will lead to blown fuse and ESIM364 alarm system will have to be repaired.
7. How do I disable SMS reports and calls in case of tamper violation when alarm system is disarmed?	The SMS reports on tamper violation can be disabled by EKB2, EKB3, EKB3W keypads or *ELDES Configuration Tool* software. For mor details, please refer to **16. TAMPERS** or to the software's HELP section. However, due to security reasons it is not recommended to disable this feature.

Question	Answer
8. Is any additional configuration necessary when connecting EPGM1 module after wiring is done accroding to EPGM1 user manual?	No additional configuration is required in order to make EPGM1 module operational.
9. Does the number of EPGM1 zones duplicate when ATZ mode is activated in the system?	No, the number of EPGM1 zones does not duplicate in ATZ mode as EPGM1 module does not support ATZ mode. Only ESIM364 zones duplicate in ATZ mode.
10. I connect the wired siren to ESIM364 and I hear a silent sound alarm even when the alarm system is disarmed. In case of alarm system alarm the siren provides a loud sound alarm as it should. Why?	Please, connect the resistor of 3,3 kΩ nominal to the BELL- / BELL+ contacts This should solve the problem.
11. I am using Windows operating system. The windows of *ELDES Configuration Tool* are not fully displayed and some parts are like cut-off. What's wrong?	Please, update *ELDES Configuration Tool* software by visiting www.eldes.lt/en/download and downloading the latest version.
12. The buzzer remains active when I disarm the alarm system using the keypad. Why?	The buzzer is intended for iButton indication only and it is not related to disarming process by keypad.
13. One of wireless devices connected to ESIM364 system sends a tamper alarm from time to time, although no tamper was violated. Why?	This happens due to wireless connection loss. There might be several reasons: 1. ELDES wireless device is installed too close or too far from ESIM364 system. 2. Interference of other electronic equipment. 3. Physical interference (building walls, floors etc.) 4. Metal material interference.
14. I have connected a wired magnetic door sensor, but I receive tamper alarm instead of zone alarm. What's wrong?	This happens due to incorrect resistor connection. Please, refer to corresponding connection circuit according to the selected zone connection type (Type 1 – 5). See **2.3.2 Zone Connection Types** for more details.
15. I disconnected the backup battery, but did not receive any SMS report on this event. How do I enable SMS report on backup battery disconnection?	By default, this notification is enabled. The system checks the backup battery resistance once a day and sends an SMS report to User 1 on backup battery replacement if more than 2Ω resistance is detected. For more details, please refer to **21. BACKUP BATTERY, MAINS POWER SUPPLY STATUS MONITORING AND MEMORY.**
16. When I check system SIM card credit balance I see a lot of SMS delivery confirmation reports. How do I disable SMS delivery confirmation ESIM364 system?	Every time an SMS text message is sent to the user, the system must "know" that the message was successfully delivered. The only way to partly disable the SMS delivery report (for alarm notifications only) is to enable alarm SMS notifications to all users. This is useful when having only User1 phone number set up, as in case of alarm the system sends the alarm SMS text message to all preset users simultaneously, but does not require any SMS delivery report.
17. I have set zone names and/or PGM output names containing some Cyrillic and/or non-English characters. The zone names and PGM output names do not fully fit in the SMS message. What's wrong?	According to GSM standards 1 SMS text message may consist of up to 160 Latin alphabet/English characters maximum. If the message contains at least one non-latin/non-English character, the length of SMS message becomes at least half shorter, since those characters occupy more size of the SMS text message than the Latin ones. It is recommended not to use any non-Latin/ non-English characters in zone names and PGM output names.
18. The configuration of added wireless keyfob EWK1 to ESIM364 system is not visible in *ELDES Configuration Tool*. What's wrong?	*ELDES Configuration Tool* version is too old. Please, update it.
19. I am unable to run *ELDES Configuration Tool* - I receive error messages in Windows. Why?	Microsoft .NET Framework v3.5 is not installed in Windows system. Please, download this package from official Microsoft website free of charge and install it to your Windows system.
20. Info SMS report comes with wrong date and time. How do I correct it?	Please, set the correct system date and time using either *ELDES Configuration Tool*, EKB2, EKB3, EKB3W or SMS text message.
21. I receive an error message when attempting to configure the device or update the firmware remotely. Whats wrong?	It appears that the device is unable to establish a communication with configuration / FTP server. Please, check the GPRS settings in ESIM364 configuration (APN, user name, password), the location of the firmware ..bin file (must be located in the FTP server folder titled **Firmware**) and the mobile internet feature presence on the SIM card used with ESIM364. If this does not solve the problem, please contact your GSM operator (and ISP - for remote configuration problems) in order to request a list of blocked TCP ports.
22. I waited for at least 5 minutes, but did not receive any SMS message confirming that remote configuration via GPRS connection has stopped. What's wrong?	1. Send the *ssss_endconfig* SMS text message. 2. In *ELDES Configuration Tool* software press Disconnect button and repeat the steps from the beginning as described in **5.4. ELDES Configuration Tool Software**
23. The SMS password is changed and I have User 1 phone number added. However, whenever I send a text message, such as XXXX INFO the system always replies with „Wrong password". What's wrong?	Most likely you have wrong character encoding set up in your SMS text messaging settings on your smart-phone. Please, ensure that you have GSM Alphabet selected, NOT Unicode or any other type of character encoding.

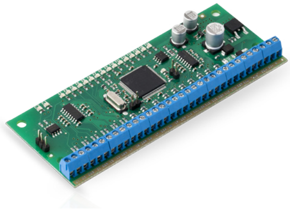
39. RELATED PRODUCTS

EKB2 - LCD keypad

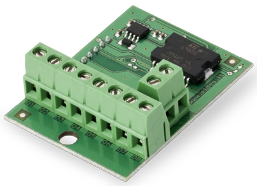
EKB3 - LED keypad



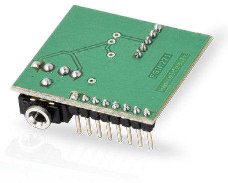
ME1 - metal cabinet



EPGM1 - hardwired zone and PGM output expansion module



EPGM8 - hardwired PGM output expansion module



EA1 - audio output module

EA2 - audio output module with amplifier

DS1990A-F5 - iButton key

DS18S20 - temperature sensor

ED1T - plastic enclosure with iButton key reader and temperature sensor

EWP1 - wireless PIR sensor (motion detector)

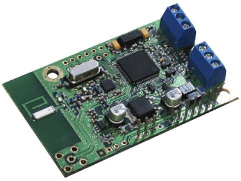
EWD1 - wireless magnetic door contact

EWS2 - wireless external siren

EWS1 - wireless internal siren

EWK1 - wireless keyfob

EWF1 – wireless smoke detector



EW1 - wireless zone and PGM output expansion module

EW1B - battery-powered wireless zone and PGM output expansion module

EKB3W – wireless LED keypad

EWK2 - wireless keyfob

EWD2 - wireless door contact/shock sensor

EWS3 - wireless indoor siren

Made in the European Union
www.eldes.lt